JIS B 9705-1 (2011) (Japanese): Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design

BLANK PAGE





JIS

機械類の安全性－制御システムの安全関連部－第１部：設計のための一般原則

JIS B 9705-1：2011

(ISO 13849-1：2006)

(JMF)

平成 23 年 7 月 25 日 改正

日本工業標準調査会 審議

(日本規格協会 発行)

日本工業標準調査会標準部会 産業機械技術専門委員会 構成表

	氏名	所属
（委員会長）	小 林 英 男	横浜国立大学
（委員）	石 坂 　 清	社団法人日本機械工業連合会
	市 川 直 樹	独立行政法人産業技術総合研究所
	梅 崎 重 夫	独立行政法人労働安全衛生総合研究所
	岡 田 　 博	日本内燃機関連合会
	奥 山 正 二	社団法人日本産業機械工業会
	狩 野 文 雄	東京都健康安全研究センター（社団法人日本空気清浄協会）
	酒 井 健 二	東洋エンジニアリング株式会社
	眞 田 一 志	横浜国立大学（社団法人日本フルードパワー工業会）
	中 山 良 樹	株式会社やまびこ（社団法人日本農業機械工業会）
	橋 本 恭 典	社団法人全国木工機械工業会
	森 　 吉 尚	国土交通省
	山 名 　 良	社団法人日本建設機械化協会

主 務 大 臣：厚生労働大臣，経済産業大臣　　制定：平成 12.11.20　　改正：平成 23.7.25
官 報 公 示：平成 23.7.25
原 案 作 成 者：一般社団法人日本機械工業連合会
（〒105-0011　東京都港区芝公園 3-5-8　機械振興会館　TEL 03-3434-9436）
審 議 部 会：日本工業標準調査会　標準部会（部会長　稲葉　敦）
審議専門委員会：産業機械技術専門委員会（委員会長　小林　英男）

この規格についての意見又は質問は，上記原案作成者，厚生労働省労働基準局 安全衛生部安全課［〒100-8916　東京都千代田区霞が関 1-2-2　TEL 03-5253-1111（代表）］又は経済産業省産業技術環境局 基準認証ユニット産業基盤標準化推進室［〒100-8901　東京都千代田区霞が関 1-3-1　TEL 03-3501-1511（代表）］にご連絡ください。

なお，日本工業規格は，工業標準化法第 15 条の規定によって，少なくとも 5 年を経過する日までに日本工業標準調査会の審議に付され，速やかに，確認，改正又は廃止されます。

目　次

ページ

日本工業規格　　　　　　　　　JIS
B 9705-1：2011

機械類の安全性－制御システムの安全関連部－第１部：設計のための一般原則

正　誤　票

区分	位置	誤	正
本体	**表 2** 記号及び略号 I，I1，I2 の定義及び記載箇所の欄	**5.2**	**6.2**
附属書 C	**表 C.1** 接触器　定格負荷の代表値の欄	B_{10d}＝20 000 00	B_{10d}＝2 000 000
	表 C.1 位置スイッチ（別のアクチュエータ，施錠装置付き）負荷の考慮なしの代表値の欄	B_{10d}＝20 000 00	B_{10d}＝2 000 000
附属書 D	**D.1** 式(D.1)	$\frac{1}{MTTF_d}=\sum_{i=1}^{\tilde{N}}\frac{1}{MTTF_{di}}=\sum_{i=1}^{\tilde{N}}\frac{n_j}{MTTF_{dj}}$	$\frac{1}{MTTF_d}=\sum_{i=1}^{\tilde{N}}\frac{1}{MTTF_{di}}=\sum_{j=1}^{\tilde{N}}\frac{n_j}{MTTF_{dj}}$
	表 D.1 J の 5 のコンポーネントの欄	電磁接触器（定格負荷，**C.1** 参照）（B_{10d}＝20 000 000 サイクル，n_{op}＝633 600）	電磁接触器（定格負荷，**C.1** 参照）（B_{10d}＝2 000 000 サイクル，n_{op}＝633 600）
	D.2 式(D.2)	誤 $MTTF_d=\frac{2}{3}MTTF_{dC1}+MTTF_{dC2}=\frac{1}{\frac{1}{MTTF_{dC1}}+\frac{1}{MTTF_{dC2}}}$	正 $MTTF_d=\frac{2}{3}\left[MTTF_{dC1}+MTTF_{dC2}-\frac{1}{\frac{1}{MTTF_{dC1}}+\frac{1}{MTTF_{dC2}}}\right]$
附属書 I	**I.3.2**	各チャネル…，**附属書 C**，**附属書 D**，及び**附属書 F** に…見積る。	各チャネル…，**附属書 C**，**附属書 D**，**附属書 E** 及び**附属書 F** に…見積る。
	I.3.2 式(I.1)	$\frac{1}{MTTF_d}+\frac{1}{MTTF_{SW1A}}+\frac{1}{MTTF_{K1A}}=\cdots$	$\frac{1}{MTTF_d}=\frac{1}{MTTF_{SW1A}}+\frac{1}{MTTF_{K1A}}=\cdots$
	I.4.2 式(I.2)	$\frac{1}{MTTF_{dC1}}+\frac{1}{MTTF_{dK1B}}$	$\frac{1}{MTTF_{dC1}}=\frac{1}{MTTF_{dK1B}}$

区分	位置	誤
附属書 I	**I.4.2** 式(I.3)	$\frac{1}{MTTF_{dC2}}+\frac{1}{MTTF_{dSW2}}+\frac{1}{MTTF_{dPLC}}+\frac{1}{MTTF_{dCC}}=\cdots$
		正
		$\frac{1}{MTTF_{dC2}}=\frac{1}{MTTF_{dSW2}}+\frac{1}{MTTF_{dPLC}}+\frac{1}{MTTF_{dCC}}=\cdots$

平成 24 年 8 月 1 日作成

まえがき

この規格は，工業標準化法第 14 条によって準用する第 12 条第 1 項の規定に基づき，社団法人日本機械工業連合会（JMF）から，工業標準原案を具して日本工業規格を改正すべきとの申出があり，日本工業標準調査会の審議を経て，厚生労働大臣及び経済産業大臣が改正した日本工業規格である。

これによって，**JIS B 9705-1**:2000 は改正され，この規格に置き換えられた。

この規格は，著作権法で保護対象となっている著作物である。

この規格の一部が，特許権，出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。厚生労働大臣，経済産業大臣及び日本工業標準調査会は，このような特許権，出願公開後の特許出願及び実用新案権に関わる確認について，責任はもたない。

白　　紙

日本工業規格　　　　　　　　　　　　JIS
B 9705-1：2011
(ISO 13849-1：2006)

機械類の安全性－制御システムの安全関連部－第1部：設計のための一般原則

Safety of machinery—Safety-related parts of control systems—
Part 1: General principles for design

序文

この規格は，2006年に第2版として発行された**ISO 13849-1**を基に，技術的内容及び対応国際規格の構成を変更することなく作成した日本工業規格である。

なお，この規格で点線の下線を施してある参考事項は，対応国際規格にはない事項である。

この規格が属する機械類の安全性規格群は，**JIS B 9700-1**に示すとおり次の規格体系で構成される。

タイプA規格（基本安全規格）－全ての機械類に適用できる基本概念，設計原則及び一般的側面を規定する規格

タイプB規格（グループ安全規格）－広範な機械類に適用できる安全面又は安全防護物を規定する規格

タイプB1規格－特定の安全面（例えば，安全距離，表面温度，騒音）に関する規格

タイプB2規格－安全防護物（例えば，両手操作制御装置，インタロック装置，圧力検知装置，ガード）に関する規格

タイプC規格（個別機械安全規格）－個々の機械又は機械群の詳細な安全要求事項を規定する規格

JIS B 9705-1は，**JIS B 9700-1**に示すとおりタイプB1規格である。

タイプC規格の規定がタイプA規格又はタイプB規格から逸脱する場合，タイプC規格の規定に従って設計及び製作された機械に対しては，タイプC規格の規定がタイプA規格又はタイプB規格に優先する。

JIS B 9705-1は，制御システムの設計及び査定に関係する人，及びタイプB2規格又はタイプC規格を開発する人に対する指針を与えることを意図している。

機械における全般的リスク低減戦略の一部として，設計者は，一つ以上の安全機能をもつ安全防護物の使用によるリスク低減のための方策を選択して達成することになる。

安全機能を提供するために割り当てられる機械の制御システムの部分は，制御システムの安全関連部（SRP/CS）と呼ばれ，ハードウェア及びソフトウェアで構成することができ，かつ，これらは機械の制御システムから分離又はその統合部分とすることができる。SRP/CSは，安全機能を提供することに追加して，更に運転機能を提供する場合もある（例えば，プロセス始動の手段としての両手操作制御器）。

予見可能な条件下での制御システムの安全機能の遂行能力は，5通りのレベルのうちの一つに振り分けられて，それはパフォーマンスレベルPLと呼ばれる。このパフォーマンスレベルは，単位時間当たりの危険側故障発生確率の用語で定義される（**表3**参照）。

安全機能の危険側故障発生確率は，ハードウェア並びにソフトウェアの構造，障害検出機構の程度［診断範囲（DC）］，コンポーネントの信頼性［平均危険側故障時間（$MTTF_d$），共通原因故障（CCF）］，設計

プロセス，運転ストレス，環境条件及び運転手順を含む幾つかの要因による。

設計者を支援し，かつ，達成した PL の査定を容易にするために，この規格では，指定の設計基準及び障害条件下での指定の挙動に従った構造分類に基づく方法論を採用する。この分類は，5 通りのレベルのうちの一つに振り分けられ，それはカテゴリ B，1，2，3，4 と呼ばれる。

パフォーマンスレベル及びカテゴリは，次のような制御システムの安全関連部に適用することができる。

－ 保護装置（例えば，両手操作制御装置，インタロック装置），電気的検知保護装置（例えば，光電カーテン），圧力検知装置
－ 制御ユニット（例えば，制御機能の論理ユニット，データ処理，監視など）
－ 動力制御要素（例えば，リレー，バルブなど）

また，あらゆる種類の機械類－単純な据付装置（例えば，小さな調理用機械，又は自動ドア及びゲート）から製造用の据付装置（例えば，包装機械，印刷機械，プレス機械）まで－における安全機能実行の制御システムに適用することができる。

この規格は，SRP/CS（及び機械）の用途に関する設計及び性能を，例えば，第三者機関によって，自社によって，又は独立の試験先によって査定できる明確な基礎を提供することを意図している。

この規格及び **JIS B 9961** は，機械類の安全関連制御システムの設計及び実装のための要求事項を規定する。これらの規格は，その適用範囲に従っていずれを使用しても関連の必須安全要求事項を満たすということが想定される。**表 1** は，この規格 **JIS B 9705-1** 及び **JIS B 9961** の範囲を要約したものである。

表 1－この規格及び JIS B 9961 の適用のための推奨情報

	安全関連制御機能実装の技術方式	**JIS B 9705-1**	**JIS B 9961**
A	非電気式，例えば液圧式	×	適用できない。
B	電気機械式，例えば，リレー，及び／又は非複雑電子システム	PL e までの指定のアーキテクチャ [a] に適用。	SIL3 までの全てのアーキテクチャに適用。
C	高複雑度電子システム，例えば，プログラム式	PL d までの指定のアーキテクチャ [a] に適用。	同上
D	A と B との複合	PL e までの指定のアーキテクチャ [a] に適用。	X [c]
E	C と B との複合	PL d までの指定のアーキテクチャ [a] に適用。	SIL3 までの全てのアーキテクチャに適用。
F	C と A，又は C と A 及び B との複合	X [b]	X [c]

X 見出しに示される規格によって取り扱われるアイテムを示す。

注 [a] 指定のアーキテクチャは，この規格の **6.2** に示され，PL の定量化に関する簡単化した手法が与えられる。
[b] 高複雑度電子システムには，この規格に指定される PL d までのアーキテクチャ又は **JIS B 9961** によるアーキテクチャを用いることができる。
[c] 非電気的な制御システムには，サブシステムとしてこの規格に適合する部品を用いる。

1 適用範囲

この規格は，ソフトウェアの設計を含み，制御システムの安全関連部（SRP/CS）の設計及び統合のための原則に関する安全要求事項及び指針について規定する。SRP/CS に対して，この規格は，安全機能を実行するために要求されるパフォーマンスレベルを含む特性を規定する。この規格は，全ての機械類に対して，用いられるテクノロジー（技術方式）及びエネルギーの形式（例えば，電気，液圧，空圧，機械）にかかわらず，SRP/CS に適用される。

個々のケースにおいて，いずれの安全機能及びパフォーマンスレベルを用いるかは規定しない。

この規格は，プログラマブル電子システムを使用するSRP/CSのための特定の要求事項を規定する。

この規格はSRP/CSの一部である製品の設計に対する特別な要求事項を規定しない。しかし，カテゴリ又はPLのような原則は使用することができる。

注記 1 SRP/CSの一部である製品の例は，リレー，ソレノイドバルブ，位置スイッチ，PLC（プログラマブルロジックコントローラ），モータコントロールユニット，両手操作制御装置，圧力検知装置である。これらの製品の設計に対しては，特別に適用可能な規格，例えば，**JIS B 9712**，**JIS B 9717-1**及び**ISO 13856-2**を参照することが重要である。

注記 2 要求PLの定義は，**3.1.24**参照。

注記 3 プログラマブル電子システムに対するこの規格の要求事項は，**JIS B 9961**で規定される機械の安全関連電気・電子・プログラマブル電子制御システムの設計及び開発の方法論と両立する。

注記 4 PLr（要求パフォーマンスレベル）＝eのコンポーネントの安全関連組込みソフトウェアに対しては，**IEC 61508-3**の箇条**7**参照。

注記 5 **表 1**参照。

注記 6 この規格の対応国際規格及びその対応の程度を表す記号を，次に示す。

ISO 13849-1:2006，Safety of machinery－Safety-related parts of control systems－Part 1: General principles for design（IDT）

なお，対応の程度を表す記号“IDT”は，**ISO/IEC Guide 21-1**に基づき，“一致している”ことを示す。

2 引用規格

次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。これらの引用規格は，その最新版（追補を含む。）を適用する。

JIS B 9700-1 機械類の安全性－設計のための基本概念，一般原則－第1部：基本用語，方法論

注記 対応国際規格：**ISO 12100-1**，Safety of machinery－Basic concepts, general principles for design－Part 1: Basic terminology, methodology（IDT）

JIS B 9700-2 機械類の安全性－設計のための基本概念，一般原則－第2部：技術原則

注記 対応国際規格：**ISO 12100-2**，Safety of machinery－Basic concepts, general principles for design－Part 2: Technical principles（IDT）

JIS B 9702 機械類の安全性－リスクアセスメントの原則

注記 対応国際規格：**ISO 14121**，Safety of machinery－Principles of risk assessment（IDT）

ISO 13849-2，Safety of machinery－Safety-related parts of control systems－Part 2: Validation

IEC 60050-191，International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service, Amd. 1:1999及びAmd. 2:2002

IEC 61508-3，Functional safety of electrical/electronic/programmable electronic safety-related systems－Part 3: Software requirements及びCorr.1:1999

IEC 61508-4，Functional safety of electrical/electronic/programmable electronic safety-related systems－Part 4: Definitions and abbreviations及びCorr.1:1999

3　用語，定義，記号及び略号

3.1　用語及び定義

この規格で用いる主な用語及び定義は，**JIS B 9700-1** 及び **IEC 60050-191** によるほか，次による。

3.1.1

制御システムの安全関連部，SRP/CS（safety-related parts of a control system）

安全関連入力信号に応答し，安全関連出力信号を生成する制御システムの部分。

注記 1　制御システムに組み合わされた安全関連部は，安全関連入力信号の発生するところ（例えば，位置スイッチの作用カム及びローラを含む。）で始まって，動力制御要素（例えば，接触器の主接点を含む。）の出力で終わる。

注記 2　監視システムが診断に使用される場合，これは SRP/CS と見なされる。

3.1.2

カテゴリ（category）

障害に対する抵抗性（フォールト・レジスタンス），及び障害条件下におけるその後の挙動に対する制御システムの安全関連部の特性に関する分類であって，当該部の構造的配置，障害検出及び／又はこれらの信頼性によって達成される。

3.1.3

障害（fault）

予防保全又はその他の計画的行動若しくは外部資源の不足によって機能を実行できない状態を除き，要求される機能を実行できないアイテムの状態。

注記 1　障害は，しばしばアイテム自体の故障の結果であるが，事前の故障がなくても存在することがある。

（**IEC 60050-191** の **05-01** 参照）

注記 2　この規格では，障害はランダム障害を意味する。

注記 3　障害（fault）は，**JIS B 9700-1** では“不具合（障害）”としているが，この規格で定義する障害と同じ意味である。“不具合”は主に機械に対して用いられる。

3.1.4

故障（failure）

要求される機能を遂行する能力がアイテムになくなること。

注記 1　故障後に，そのアイテムは障害をもつ。

注記 2　“故障”は事象であって，状態を示す“障害”とは異なる。

注記 3　ここに定義する概念は，ソフトウェアだけで構成されるアイテムには適用しない。

（**IEC 60050-191** の **04-01** 参照）

注記 4　制御下のプロセスのアベイラビリティにだけ影響する故障に関しては，この規格の適用範囲外である。

3.1.5

危険側故障（dangerous failure）

SRP/CS を危険状態又は機能不能状態に導く潜在性をもつ故障。

注記　故障が現実に危険側故障を導くかどうかは，システムのチャネルアーキテクチャに依存することがある。冗長システムにおいては，危険側ハードウェア故障が SRP/CS 全体を危険状態又は機能不能状態に導く可能性は少ない。

（**IEC 61508-4** の **3.6.7** から採用）

3.1.6

共通原因故障［common cause failure (CCF)］

単一の事象から生じる異なったアイテムの故障であって，これらの故障が互いの結果ではないもの。

（**IEC 60050-191 Amd. 1** の **04-23** 参照）

注記 共通原因故障は共通モード故障と混同してはならない。

3.1.7

システマティック故障（systematic failure）

何らかの原因に確定的に関係する故障であって，設計，製造プロセス，運転手順，文書又は他の関連要因を変更しなければ除去できない故障。

注記 1 変更を伴わない修理では，通常，システマティック故障の原因を除去できない。

注記 2 故障原因をシミュレートすることによって，システマティック故障を再現することができる。

（**IEC 60050-191** の **04-19** 参照）

注記 3 システマティック故障の原因の事例には，次の段階で起こす人間の過誤を含む。

- 安全要求仕様
- ハードウェアの設計，製造，据付及び運転
- ソフトウェアの設計，実装など

3.1.8

ミューティング（muting）

SRP/CS による安全機能の一時的自動中断。

3.1.9

手動リセット（manual reset）

機械の再起動に先立って，一つ以上の安全機能を手動で回復させるために用いられる SRP/CS 内の機能。

3.1.10

危害（harm）

身体的傷害又は健康障害。

（**JIS B 9700-1** の **3.5** 参照）

3.1.11

危険源（hazard）

危害を引き起こす潜在的根源。

注記 1 “危険源”という用語は，その発生源（例えば，機械的危険源，電気的危険源）を明確にし，又は潜在的な危害（例えば，感電の危険源，切断の危険源，毒性による危険源，火災による危険源）の性質を明確にするために修飾されることがある。

注記 2 この定義において，危険源は，次を想定している。

- 機械の“意図する使用”の期間中，恒久的に存在するもの（例えば，危険な動きをする要素の運動，溶接工程中の電弧，不健康な姿勢，騒音のエミッション，高温），又は
- 予期せずに現れ得るもの（例えば，爆発，意図しない／予期しない起動の結果としての押しつぶしの危険源，破損の結果としての放出，加速度又は減速度の結果としての落下）

（**JIS B 9700-1** の **3.6** 参照）

3.1.12

危険状態（hazardous situation）

人が少なくとも一つの危険源に暴露される状況。暴露されることが，直ちに又は長期間にわたり危害を引き起こす可能性がある。

（**JIS B 9700-1** の **3.9** 参照）

3.1.13

リスク（risk）

危害の発生確率と危害のひどさの組合せ。

（**JIS B 9700-1** の **3.11** 参照）

3.1.14

残留リスク（residual risk）

保護方策を講じた後に残るリスク。

図 **2** 参照。

（**JIS B 9700-1** の **3.12** から採用）

3.1.15

リスクアセスメント（risk assessment）

リスク分析及びリスクの評価を含む全てのプロセス。

（**JIS B 9700-1** の **3.13** 参照）

3.1.16

リスク分析（risk analysis）

機械の制限に関する仕様，危険源の同定及びリスク見積りの組合せ。

（**JIS B 9700-1** の **3.14** 参照）

3.1.17

リスクの評価（risk evaluation）

リスク分析に基づき，リスク低減目標を達成したかどうかを判断すること。

（**JIS B 9700-1** の **3.16** 参照）

3.1.18

機械の“意図する使用”（intended use of a machine）

使用上の指示事項の中に提供された情報に基づく機械の使用。

（**JIS B 9700-1** の **3.22** 参照）

3.1.19

合理的に予見可能な誤使用（reasonably foreseeable misuse）

設計者が意図していない使用法で，容易に予測できる人間の挙動から生じる機械の使用。

（**JIS B 9700-1** の **3.23** 参照）

3.1.20

安全機能（safety function）

故障がリスクの増加に直ちにつながるような機械の機能。

（**JIS B 9700-1** の **3.28** 参照）

3.1.21

監視（monitoring）

コンポーネント又は要素の機能を実行する能力が低下する場合，又はリスク低減機能の低下を招くような方向でプロセス条件が変化する場合，保護方策の始動を確実にする安全機能。

3.1.22

プログラマブル電子システム，PES（programmable electronic system）

制御，保護又は監視のために，その動作が一つ以上のプログラマブル電子装置に依存するシステムであって，動力源，センサ及び他の入力装置，並びに接触器及び他の出力装置のようなシステムの全ての要素を含む。

（**IEC 61508-4** の **3.3.2** から採用）

3.1.23

パフォーマンスレベル，PL（performance level）

予見可能な条件下で，安全機能を実行するための制御システムの安全関連部の能力を規定するために用いられる区分レベル。

注記　**4.5.1** 参照

3.1.24

要求パフォーマンスレベル，$\mathbf{PL_r}$（required performance level）

安全機能の各々に対し，要求されるリスク低減を達成するために適用されるパフォーマンスレベル。

図 **2** 及び **A.1** 参照。

3.1.25

平均危険側故障時間，$\mathbf{MTTF_d}$（mean time to dangerous failure）

危険側故障を生じるまでの平均時間の期待値。

（**JIS B 9961** の **3.2.34** から採用）

3.1.26

診断範囲，DC（diagnostic coverage）

診断効果の尺度であり，検出される危険側故障率（分子）と全危険側故障率（分母）の間の比として決定することができる。

注記　診断範囲は，安全関連システムの全体又は一部に対してあり得る。例えば，診断範囲は，安全関連部の全体又は一部として，例えば，センサ及び／又は論理システム及び／又は最終要素の組合せとして存在することがあり得る。

（**IEC 61508-4** の **3.8.6** から採用）

3.1.27

保護方策（protective measure）

リスク低減を達成することを意図した方策。

次によって実行される。

－　例 **1**　設計者による方策（本質的安全設計方策，安全防護及び付加保護方策，使用上の情報）及び

－　例 **2**　使用者による方策［組織（安全作業手順，監督，作業許可システム），追加安全防護物の準備及び使用，保護具の使用，訓練］

（**JIS B 9700-1** の **3.18** から採用）

3.1.28

使命時間，T_M（mission time）

SRP/CS の意図する使用を網羅する期間。

3.1.29

診断試験率，r_t（test rate）

SRP/CS において，障害を検出するための自動試験頻度であって，診断試験間隔の逆数値。

3.1.30

動作要求率，r_d（demand rate）

SRP/CS の安全に関連する動作の要求頻度

3.1.31

修復率，r_t（repair rate）

オンライン試験又はシステムの明らかな機能不良のいずれかによる危険側故障の検出と，修復又はシステム・コンポーネント交換後での運転の再起動との間の時間の逆数値。

注記 修復時間は，故障検出に必要な時間幅を含まない。

3.1.32

機械制御システム（machine control system）

機械要素の部分，オペレータ，外部制御装置又はこれらの組合せからの入力信号に応答し，かつ，機械が意図するように挙動するための出力信号を生成するシステム。

注記 機械制御システムは，全ての技術方式又は異なる技術方式の組合せ（例えば，電気・電子式，液圧式，空圧式，機械式）で使用することができる。

3.1.33

安全インテグリティレベル，SIL（safety integrity level）

電気・電子・プログラマブル電子（E/E/PE）安全関連システムに割り当てる安全機能の安全インテグリティ要求事項を指定するための区分レベル（1～4）。安全インテグリティレベル 4（SIL4）が最も高い安全インテグリティに対応し，安全インテグリティレベル 1（SIL1）が最も低い安全インテグリティに対応する。

（**IEC 61508-4** の **3.5.6** 参照）

3.1.34

制約可変言語，LVL（limited variability language）

安全要求仕様を実行するための，定義済みの，アプリケーション固有の，ライブラリ機能を結合する能力をもつ言語の形式。

（**IEC 61511-1** の **3.2.81.1.2** から採用）

注記 1 LVL の代表的な例は，**JIS B 3503** で示される。LVL には，ラダー論理，ファンクションブロック図などがある。

注記 2 LVL を用いるシステムの代表的例には，PLC がある。

3.1.35

無制約可変言語，FVL（full variability language）

多様な機能及びアプリケーションを実行する能力をもつ言語の形式。

例 C，C^{++}，アッセンブラ

（**IEC 61511-1** の **3.2.81.1.3** から採用）

注記 1 FVL を用いるシステムの代表的な例は，組込みシステムである。

注記 2 機械類の分野では，FVL は，通常，組込みソフトウェアで使われ，アプリケーションソフトウェアに使われることはまれである。

3.1.36

アプリケーションソフトウェア（application software）

機械製造業者が作成する，固有の用途に用いるソフトウェアであって，一般に SRP/CS 要求事項を満たすために必要な，適切な入力・出力・計算・決定論理を制御する論理シーケンス，限界値及び命令を含む。

3.1.37

組込みソフトウェア, ファームウェア, システムソフトウェア（embedded software, firmware, system software）

制御装置製造業者がシステムに組み込むソフトウェアであって，システムの一部であり，機械類の使用者による変更のためにアクセスできないソフトウェア。

注記 組込みソフトウェアは，通常 FVL で記述される。

3.2 記号及び略号

記号及び略号は，**表 2** による。

表 2－記号及び略号

記号及び略号	説明	定義及び記載箇所
a，b，c，d，e	パフォーマンスレベルの記号	**表 3**
AOPD	能動的光電保護装置（例えば，ライトカーテン）	**附属書 H**
B，1，2，3，4	カテゴリの記号	**表 7**
B_{10d}	コンポーネントの 10 %が危険側に故障する（空圧式及び電気機械式コンポーネント）までのサイクル数	**附属書 C**
Cat.	カテゴリ	**3.1.2**
CC	電流変換器	**附属書 I**
CCF	共通原因故障	**3.1.6**
DC	診断範囲	**3.1.26**
DC_{avg}	平均診断範囲	**E.2**
F，F1，F2	危険源に暴露される頻度及び／又は時間	**A.2.2**
FB	ファンクションブロック	**4.6.3**
FVL	無制約可変言語	**3.1.35**
FMEA	故障モード及び影響分析	**7.2**
I，I1，I2	入力装置，例えば，センサ	**5.2**
i，j	カウント用の添字	**附属書 D**
I/O	入力／出力	**表 E.1**
i_{ab}，i_{bc}	相互接続手段	**図 4**
K1A，K1B	接触器	**附属書 I**
L，L1，L2	論理	**6.2**
LVL	制約可変言語	**3.1.34**
M	モータ	**附属書 I**
MTTF	平均故障時間	**附属書 C**
$MTTF_d$	平均危険側故障時間	**3.1.25**
n，N，$\tilde{N}$	アイテムの数	**6.3**，**D.1**
N_{low}	SRP/CS の組合せにおける PL_{low} での SRP/CS の数	**6.3**
O，O1，O2，OTE	出力装置，例えば，主接触器	**6.2**
P，P1，P2	危険源回避の可能性	**A.2.3**
PES	プログラマブル電子システム	**3.1.22**
PL	パフォーマンスレベル	**3.1.23**
PLC	プログラマブルロジックコントローラ	**附属書 I**
PL_{low}	SRP/CS の組合せにおける最低のパフォーマンスレベル	**6.3**

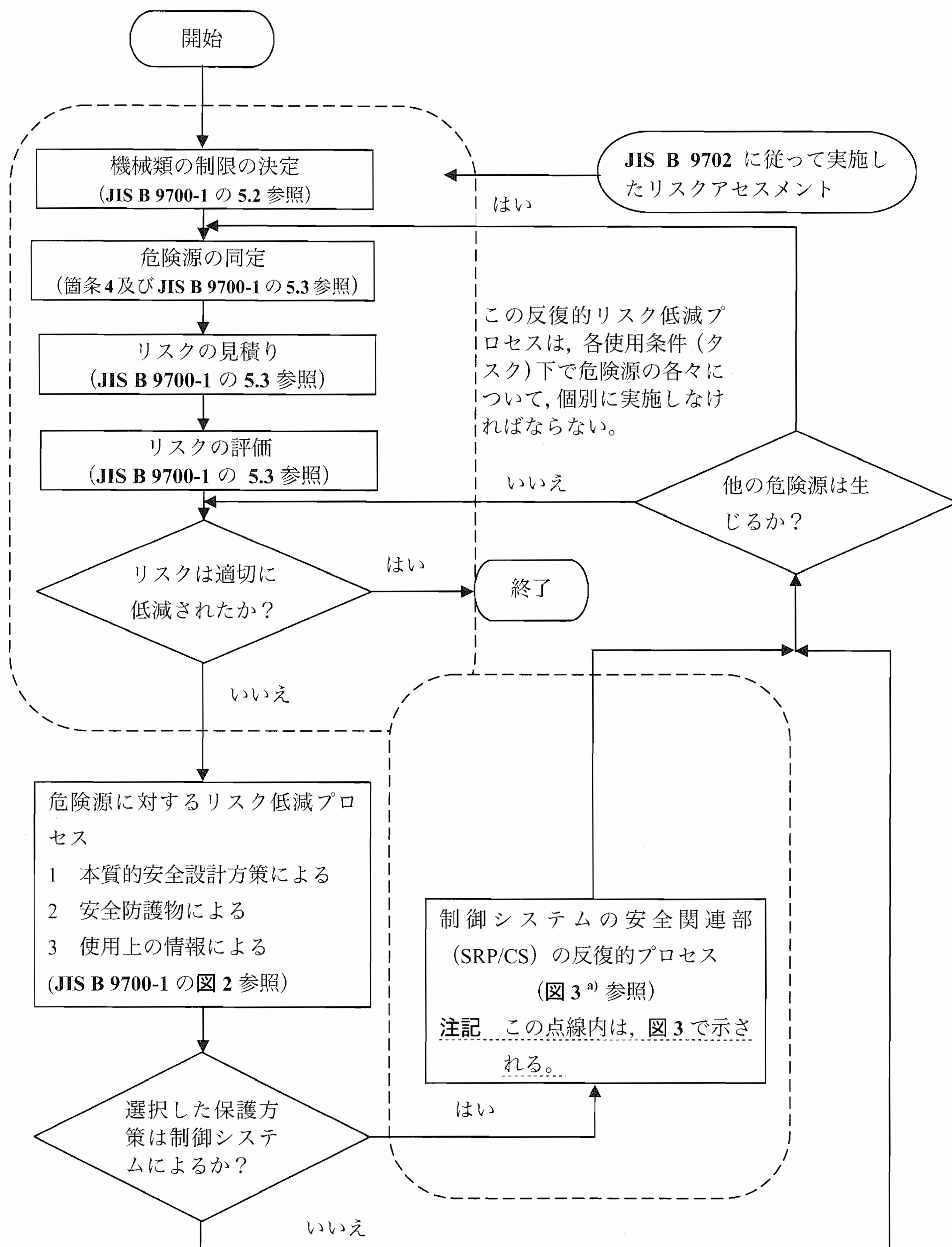
表 2－記号及び略号（続き）

記号及び略号	説明	定義及び記載箇所
PL_r	要求パフォーマンスレベル	**3.1.24**
r_d	動作要求率	**3.1.30**
RS	回転センサ	**附属書 I**
S，S1，S2	傷害のひどさ	**A.2.1**
SW1A，SW1B，SW2	位置スイッチ	**附属書 I**
SIL	安全インテグリティレベル	**表 4**
SRASW	安全関連アプリケーションソフトウェア	**4.6.3**
SRESW	安全関連組込みソフトウェア	**4.6.2**
SRP	安全関連部	**一般要求事項**
SRP/CS	制御システムの安全関連部	**3.1.1**
TE	試験装置	**6.2**
T_M	使命時間	**3.1.28**

4　設計上での考慮事項

4.1　設計における安全性の目標

SRP/CS は，**JIS B 9700-1** 及び **JIS B 9702** の原則を十分に考慮し（**図 1** 及び**図 3** 参照），設計及び製作しなければならない。全ての意図する使用及び合理的に予見可能な誤使用を考慮しなければならない。



注 a) この規格の図 3 参照

図 1－リスクアセスメント／リスク低減の概要

4.2 リスク低減のための方法論

4.2.1 一般要求事項

機械におけるリスク低減の方法論は，**JIS B 9700-1** の **5.**（リスク低減のための方法論）で規定されており，更に指針が，**JIS B 9700-2** の **4.**（本質的安全設計方策）及び **JIS B 9700-2** の **5.**（安全防護及び付加保護方策）で規定される。この方法論は機械のライフサイクル全体を網羅している。

機械の危険源分析及びリスク低減プロセスは，次の階層的方策によって危険源を除去又は低減することを要求している。

－ 設計による危険源除去又はリスク低減（**JIS B 9700-2** の **4.**参照）

－ 安全防護方策及び付加保護方策によるリスク低減（**JIS B 9700-2** の **5.**参照）

－ 残留リスクに関する使用上の情報の準備によるリスク低減［**JIS B 9700-2** の **6.**（使用上の情報）参照］

4.2.2 リスク低減に対する制御システムの寄与

機械の全般的設計手順に従うことの目的は，安全性の目標（**4.1** 参照）を達成することである。要求のリスク低減を提供する SRP/CS の設計は，機械の全般的設計手順に組み込まれた一部である。SRP/CS は，要求のリスク低減を達成する安全機能を PL として提供する。設計の本質的な安全部分として，又は安全防護物若しくは保護装置の制御部分として安全機能を提供する際，SRP/CS の設計はリスク低減の方法論の一部である。これは，反復的プロセスであり，**図 1** 及び**図 3** で示される。

個々の安全機能に対して，その特性（箇条 **5** 参照）及び要求パフォーマンスレベルは，安全要求仕様において指定され，かつ，文書化されなければならない。

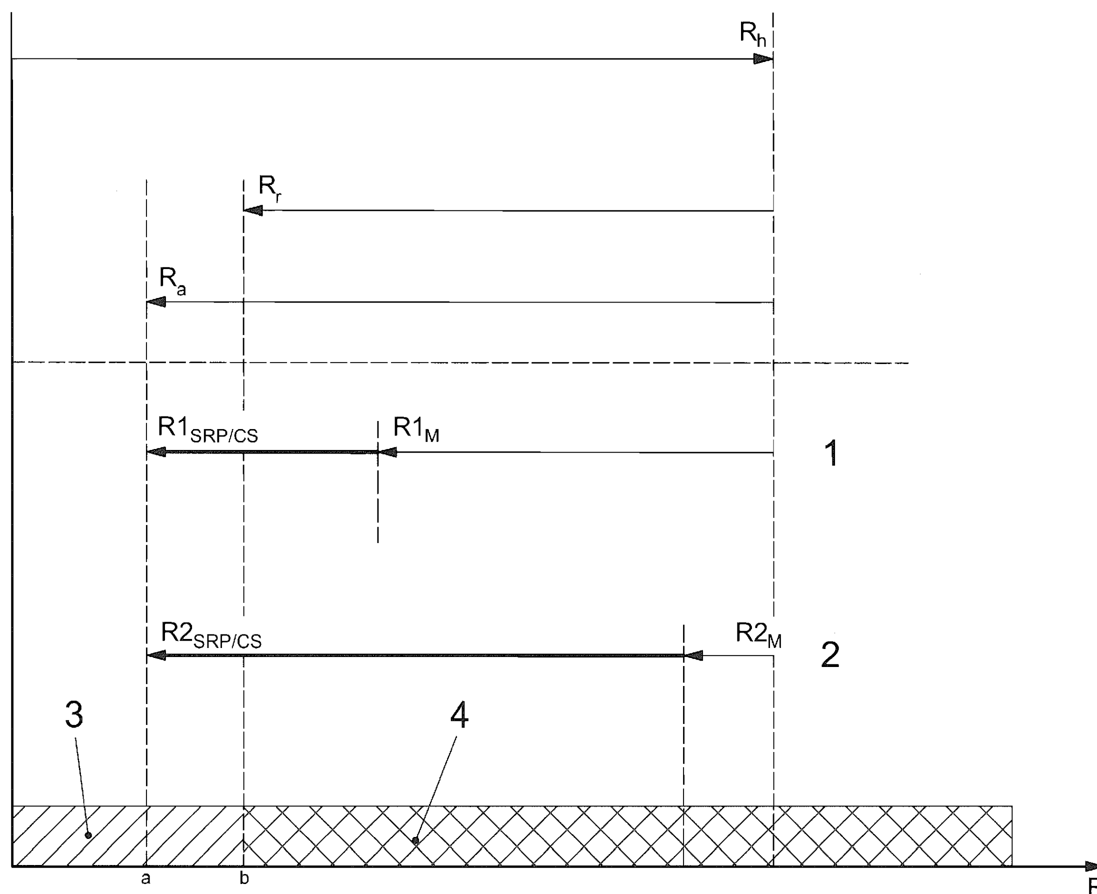
この規格においては，PL は単位時間当たりの危険側故障発生確率（Probability of a Dangerous Failure, *PFH*d）で規定される。5 通りの PL（a～e）が，単位時間当たりの危険側故障発生確率の指定範囲（**表 3** 参照）で規定される。

表 3－パフォーマンスレベル（PL）

PL	単位時間当たりの危険側故障発生の平均確率（*PFH*d）［1/h］
a	$10^{-5} \leqq PFH\mathrm{d} < 10^{-4}$
b	$3 \times 10^{-6} \leqq PFH\mathrm{d} < 10^{-5}$
c	$10^{-6} \leqq PFH\mathrm{d} < 3 \times 10^{-6}$
d	$10^{-7} \leqq PFH\mathrm{d} < 10^{-6}$
e	$10^{-8} \leqq PFH\mathrm{d} < 10^{-7}$
注記 単位時間当たりの危険側故障発生の平均確率に加えて，PL を達成するために，他の方策も必要とされる。	

機械におけるリスクアセスメント（**JIS B 9702** 参照）から，設計者は，SRP/CS によって実行される，関連のあるそれぞれの安全機能によるリスク低減への寄与度を決定しなければならない。この寄与度は，制御下の機械類の全体にわたるリスクを網羅してはいない。例えば，機械プレス又は洗濯機の全体にわたるリスクを網羅してはいないと考えられる。しかし特別な安全機能の適用によって部分的リスクは低減される。そのような機能の例は，プレスの電気的検知保護装置の使用によって開始される停止機能，又は洗濯機のドアロック機能である。

リスク低減は，種々の保護方策（SRP/CS 及び非 SRP/CS 共に）を適用することによって，所定の安全条件達成の最終結果として実現できる（**図 2** 参照）。



記号の説明

R_h　ある特定の危険状態に対する，保護方策が講じられる前のリスク

R_r　保護方策によって要求されるリスク低減量

R_a　保護方策で達成される実際のリスク低減量

1　解決策 1－SRP/CS 以外の保護方策（例えば，機械的方策）によるリスク低減が主で，SRP/CS によるリスク低減量が低い。

2　解決策 2－SRP/CS によるリスク低減（例えば，ライトカーテン）が主で，SRP/CS 以外の保護方策によるリスク低減量が低い。

3　適切に低減されたリスク

4　不適切に低減されたリスク

R　リスク

a　解決策 1 及び解決策 2 によっても残る残留リスク

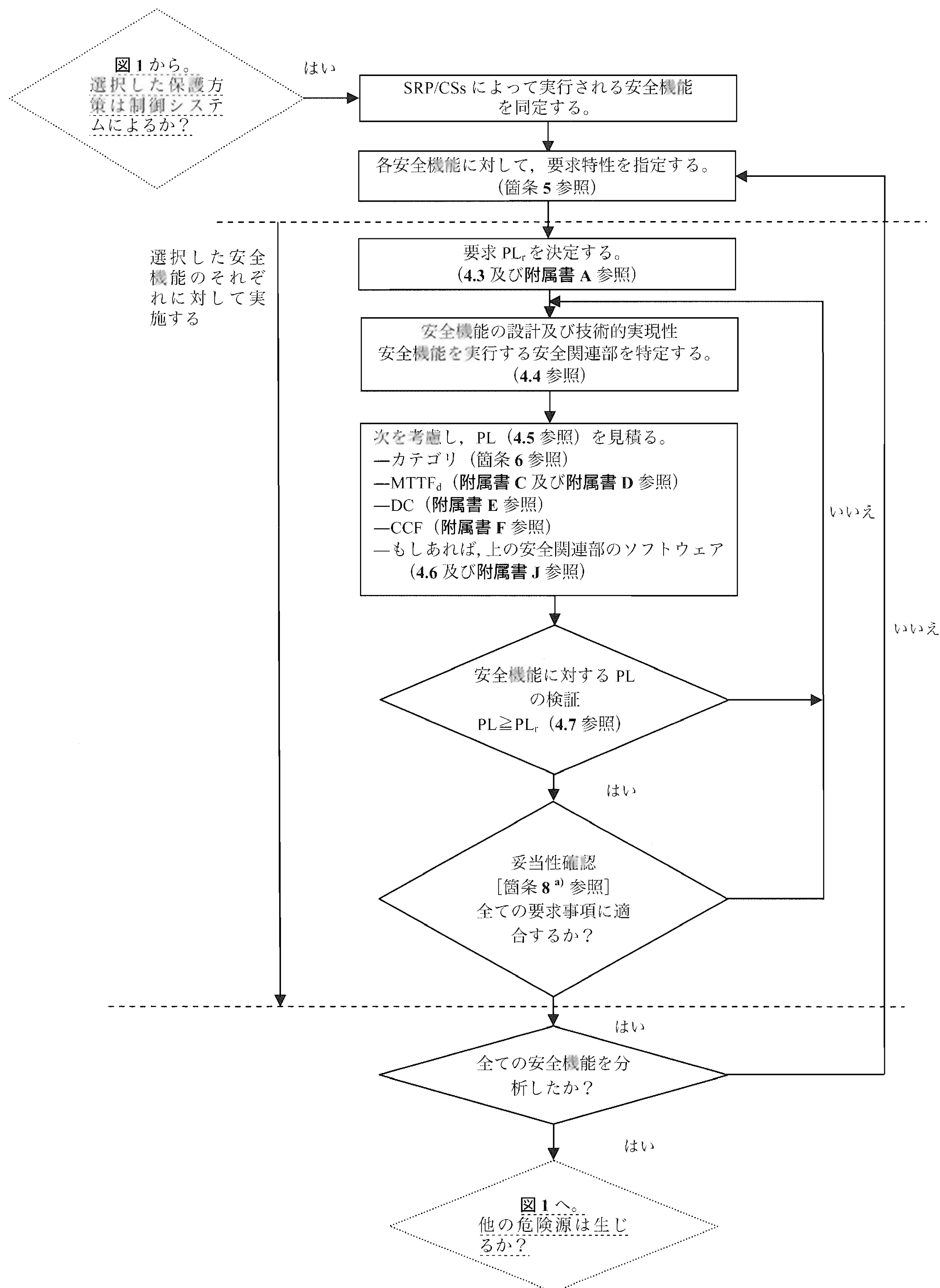
b　適切に低減されたリスク

$R1_{SRP/CS}$，$R2_{SRP/CS}$　SRP/CS によって実行される安全機能による低減リスク

$R1_M$，$R2_M$　SRP/CS 以外の保護方策（例えば，機械的方策）による低減リスク

注記　リスク低減に関する更なる情報は，**JIS B 9700** 規格群参照。

図 2－個々の危険状態に対するリスク低減プロセスの概要



注 a)　**ISO 13849-2** で，妥当性確認のための追加的支援策が示される。

図 3－制御システムの安全関連部（SRP/CS）の設計のための反復的プロセス

4.3　要求パフォーマンスレベル PL_r の決定

SRP/CS によって実行される選択したそれぞれの安全機能に対して，要求パフォーマンスレベル PL_r を決定し，かつ，文書化しなければならない（PL_r 決定に関する指針は，**附属書 A** 参照）。要求パフォーマンスレベルの決定は，リスクアセスメントの結果に従い，また制御システムの安全関連部によって実行されるリスク低減量に関わる（**図 2** 参照）。

PL_r は高くなるほど，SRP/CS によって提供されるリスク低減量は大きくなければならない。

4.4　SRP/CS の設計

リスク低減プロセスの一部は，機械の安全機能を決定することである。これは制御システムの安全機能，例えば，予期しない起動の防止を含む。

一つの安全機能は，一つ以上の SRP/CS によって実行される場合があり，かつ，複数の幾つかの安全機能は一つ以上の SRP/CS（例えば，論理ユニット，動力制御要素）に分割される場合がある。一つの SRP/CS が安全機能及び通常の制御機能を実行することが可能である。設計者は，有効な技術方式のいずれかを単独又は組み合せて用いることが望ましい。また，SRP/CS は操作機能（例えば，サイクル開始の手段としての AOPD）を提供する場合もある。

代表的な安全機能は，**図 4** のダイアグラムで表現され，制御システムの安全関連部（SRP/CS）は次の組合せによる。

－　入力（SRP/CS_a）

－　論理／処理（SRP/CS_b）

－　出力／動力制御要素（SRP/CS_c）

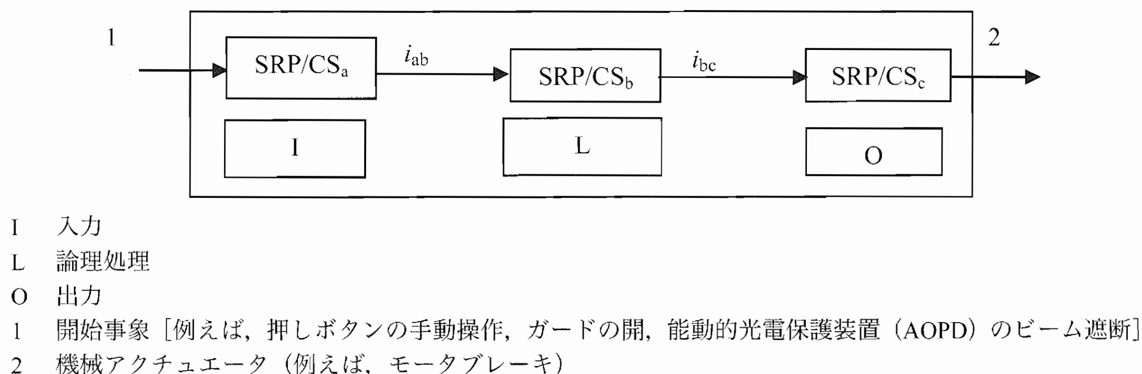
－　相互接続手段（i_{ab}，i_{bc}）（例えば，電気的，光学的）

注記 1　同一の機械類内で，種々の安全機能とそれらに関連する SRP/CS が実行する特定の安全機能を区別することは重要である。

制御システムの安全機能を同定する場合，設計者は SRP/CS（**図 1** 及び**図 3** 参照）を特定しなければならない。また，必要な場合，入力，論理及び出力に SRP/CS を割り当て，また，冗長系の場合には，個々のチャネルに対して SRP/CS を割り当て，その後，パフォーマンスレベル PL を評価しなければならない。

注記 2　指定のアーキテクチャは，箇条 **6** で示される。

注記 3　全ての相互接続手段は，安全関連部に含まれる。



I　入力
L　論理処理
O　出力
1　開始事象［例えば，押しボタンの手動操作，ガードの開，能動的光電保護装置（AOPD）のビーム遮断］
2　機械アクチュエータ（例えば，モータブレーキ）

図 4－代表的な安全機能を処理するための制御システムの安全関連部の組合せに関するダイアグラム

4.5　達成されるパフォーマンスレベル PL の評価と SIL との関係

4.5.1　パフォーマンスレベル PL

この規格においては，安全関連部が安全機能を遂行する能力は，パフォーマンスレベルの決定によって表される。

安全機能を遂行するために選択したSRP/CSの各々及び／又はSRP/CSの組合せに対して，PLの見積りを実施しなければならない。

SRP/CSのPLは，次のパラメータを見積ることによって決定しなければならない。

- 単一チャネルの$MTTF_d$の値（**附属書C**及び**附属書D**参照）
- DC（診断範囲）（**附属書E**参照）
- CCF（共通原因故障）（**附属書F**参照）
- 構造（**箇条6**参照）
- 障害条件下の安全機能の挙動（**箇条6**参照）
- 安全関連ソフトウェア（**4.6**及び**附属書J**参照）
- システマティック故障（**附属書G**参照）
- 予期される環境条件下での安全機能遂行能力

注記1 他のパラメータ，例えば，運転局面，動作要求率，診断試験率も影響する可能性がある。

これらのパラメータは，評価プロセスに関連して二つのアプローチによってグループ化できる。

a) 定量化の側面（単一コンポーネントの$MTTF_d$値，DC，CCF，構造）

b) SRP/CSの挙動に影響を与える非定量，定性的側面（障害条件下での安全機能の挙動，安全関連ソフトウェア，システマティック故障及び環境条件）

定量化可能な側面のうち，信頼性（例えば，$MTTF_d$，構造）の寄与度は使用される技術によって変化し得る。例えば，一つの技術方式で信頼性の高い安全関連部の単一チャネルは，他の技術方式による低い信頼性のフォールトトレラント構造で同程度又はそれ以上のPLを提供することは（ある制限内で）可能である。

システムのタイプによって（例えば，複雑構造），PLの定量可能な側面を見積るための方法は，例えば，マルコフモデル，一般化確率ペトリネット（GSPN），信頼性ブロックダイアグラムのように複数存在する（例えば，**IEC 61508**規格群参照）。

PLの定量化の側面の査定をより容易にするために，この規格は，特定の設計基準及び障害条件下での挙動を満たす5通りの指定アーキテクチャを定めることによって，単純化した方法を示す（**4.5.4**参照）。

箇条6の要求事項に従って設計された単一SRP/CS又はSRP/CSの組合せに対して，危険側故障発生の平均確率は，**図5**の手段によって，及び**附属書A**～**附属書H**，**附属書J**及び**附属書K**の手順によって，見積ることができる。

指定アーキテクチャから逸脱するSRP/CSに対しては，要求パフォーマンスレベルPL_rの達成を証明するための詳細な計算を示さなければならない。

SRP/CSが単純であり，要求パフォーマンスレベルがa～cの用途に対しては，PLの定性的見積りは，設計の論理的根拠を示すことで正当化できる場合がある。

注記2 安全機能をPES（プログラマブル電子システム）のような複雑な制御システムで遂行する場合，その設計に対しては，他の規格の適用が適切である（例えば，**IEC 61508**規格群，**JIS B 9961**又は**JIS B 9704**規格群）。

PLの定性的側面の達成は，**4.6**及び**附属書G**で示される推奨方策を適用することによって証明することができる。

IEC 61508規格群に従う規格では，安全関連制御システムが安全機能を遂行する能力は，SILとして示

される。**表 4** は，PL 及び SIL に関して両概念の関係を示している。

PLa は SIL のスケールとは合わず，主に軽微なリスク，通常は回復可能な傷害を低減するために使用される。SIL4 は，プロセス産業における悲劇的な事象に対して割り当てられ，この範囲は機械のリスクには関係がない。SIL3 に対応する PLe は最も高いレベルとして定義される。

表 4－パフォーマンスレベル（PL）と安全インテグリティレベル（SIL）との関係

PL	SIL 高／継続運転モード
a	－
b	1
c	1
d	2
e	3

したがって，リスクを低減するための保護方策は，主として，次によらなければならない。

－　コンポーネントレベルでの障害発生確率の低減

　この目的は，安全機能に影響を与える障害発生確率又は故障の発生確率を低減することである。これは，コンポーネントの信頼性を向上させること，例えば，重要な障害又は故障を，低減又は除去するために，“十分吟味されたコンポーネント”の選択によって及び／又は“十分吟味された安全原則”を適用することによって達成可能である（**ISO 13849-2** 参照）。

－　SRP/CS の構造を改良する。

　この目的は，障害の危険な影響を回避することである。幾つかの障害は検知される場合があり，かつ，冗長及び／又は監視構造が必要となる。

両方策は，個別に又は組み合わせて使用することができる。技術方式によって，リスク低減は信頼性のあるコンポーネントの選択によって，及び障害の除外によって達成することができる。しかし，他の技術方式では，リスク低減は，冗長及び／又は監視システムを必要とする場合がある。追加して，共通原因故障（CCF）を考慮しなければならない（**図 3** 参照）。

アーキテクチャの制約に対しては，**箇条 6** 参照。

4.5.2　各チャネルの平均危険側故障時間（$MTTF_d$）

各チャネルの $MTTF_d$ 値は，3 通りのレベルで示される（**表 5** 参照）。また，各チャネル（例えば，単一チャネル，冗長システムの各チャネル）を個別に考慮しなければならない。

$MTTF_d$ では，100 年の最大値を考慮しなければならない。

表 5－各チャネルの平均危険側故障時間

$MTTF_d$	
各チャネルの指定表示	各チャネルの範囲
“低”	3 年≦$MTTF_d$＜10 年
“中”	10 年≦$MTTF_d$＜30 年
“高”	30 年≦$MTTF_d$＜100 年

注記 1 各チャネルの $MTTF_d$ の範囲選択は，現在の技術水準としてその分野で見られる故障率に基づいており，PL のログスケールに対応して類似のログスケールを形成する。3 年未満の各チャネルの $MTTF_d$ 値は，現実の SRP/CS で起こり得るということは予想していない。市場の全てのシステムのうちおよそ 30 %が，1 年後に故障し，かつ，取り替えることになるということを意味するからである。100 年を超えるの各チャネルの $MTTF_d$ 値は，受け入れ不可能である。理由は，高リスク対応の SRP/CS は，コンポーネントの信頼性だけに依存しないほうがよいからである。システマティック故障及びランダム故障に対して SRP/CS を強化するためには，冗長系，かつ，試験付きのような追加手段を必要とすることが望ましい。実用的には，$MTTF_d$ の範囲は，3 通りに制限される。各チャネルにおける $MTTF_d$ 値を最大 100 年に制限することは，安全機能を実行する当該 SRP/CS の単一チャネルに対して適用される。より高い $MTTF_d$ 値は，単一コンポーネントで使用することができる（**表 D.1** 参照）。

注記 2 この表の各チャネル間のしきい値は，5 %の誤差範囲内を想定している。

コンポーネントの $MTTF_d$ の見積りに対して，データを探す際は，**a)**による。ただし，これによれない場合は，**b)**によってもよい。**b)**によれない場合は，**c)**によってもよい。

a) 製造業者のデータの使用

b) **附属書 C** 及び**附属書 D** に示される方法の使用

c) $MTTF_d$ 値として 10 年を選択

4.5.3 診断範囲

DC 値は，**表 6** に示す 4 通りのレベルで示される。

DC の見積りに対しては，大抵の場合，FMEA（**IEC 60812** 参照）又は類似の方法を使用することができる。この場合，全ての関連障害及び／又は故障モードを考慮し，かつ，安全機能を遂行する SRP/CS の組合せの PL を要求パフォーマンスレベル PL_r に対して確認することが望ましい。DC を見積るための単純化したアプローチは，**附属書 E** 参照。

表 6－診断範囲

DC	
DC の指定表示	DC の範囲
“なし”	DC＜60 %
“低”	60 %≦DC＜90 %
“中”	90 %≦DC＜99 %
“高”	99 %≦DC

注記 1 複数の部分で構成される SRP/CS では DC に対して，平均の DC（DCavg）を，**図 5**，箇条 **6** 及び**附属書 E** の **E.2** に示すように使用する。

注記 2 DC の範囲の選択は，60 %，90 %及び 99 %のキー値に基づく。これは試験の診断範囲を扱う他の規格（例えば，**IEC 61508** 規格群）でも設定される。特徴として，DC 自体ではなく（100－DC）%の計測の方が試験の効果に対して有効であるということが，調査によって示される。キー値の 60 %，90 %及び 99 %に対する（100－DC）%は，PL のログスケール対応の類似のログスケールを形成する。60 %未満の DC 値は，試験のシステムの信頼性に関して僅かな効果しか有しない。したがって，“なし”とする。複雑なシステムに対する 99 %以上の DC 値は，達成することが困難である。実用的には，範囲数は，4 通りに制限される。この表の各 DC のしきい値は，5 %の誤差内を想定する。

4.5.4 PL 見積り手順の単純化

PL は，全ての関連パラメータ及び適切な計算方法を考慮し，見積ることができる（**4.5.1** 参照）。

この箇条は，指定アーキテクチャに基づく SRP/CS の PL を見積るための単純化した手順を述べる。

類似の構造をもつ他の幾つかのアーキテクチャは，PL の見積りを行うために，指定アーキテクチャに変形する必要が生じる場合がある。

指定アーキテクチャは，ブロックダイアグラムとして表し，かつ，**6.2** において各カテゴリのなかで示される。ブロックメソッド及び安全関連ブロックダイアグラムに関する情報は，**6.2** 及び**附属書 B** で示される。

指定アーキテクチャは，各カテゴリに対してシステム構造の論理的表現を示す。技術的な実現，又は，例えば，機能的回路図は，見た目には完全に異なって見える場合がある。

組合せの SRP/CS について，安全関連信号の開始点で起動して，動力制御要素（**JIS B 9700-1** の**附属書 A** 参照）の出力で終了するように，指定アーキテクチャは描いている。指定アーキテクチャは，また，入力信号に応答して，かつ，安全関連出力信号を生成する制御システムの一部又はサブシステムを記述するためにも使用できる。このように，入力要素（センサ）は，例えば，制御論理要素の入力回路又は入力スイッチと同様にライトカーテン（AOPD）とすることができる。さらに，出力要素は，例えば，出力信号開閉装置（OSSD）又はレーザスキャナの出力部とすることができる。

指定アーキテクチャに対しては，次の代表的な仮定がなされる。

- 使命時間，20 年（箇条 **10** 参照）
- 使命時間内での定故障率
- カテゴリ 2，動作要求率≦1/100 の診断試験率
- カテゴリ 2，$MTTF_{d,TE}$ は，$MTTF_{d,L}$ の 1/2 より大きい

注記 各チャネルのブロックを分離できない場合，次を適用することができる。

概略化した試験チャネル（TE：試験装置，OTE：出力試験装置）の $MTTF_d$ は，概略化した機能チャネル（I，L，O）の 1/2$MTTF_d$ より大きい。

この方法論では，カテゴリは規定の平均診断範囲 DC_{avg} をもつアーキテクチャとして考慮している。各 SRP/CS の PL は，アーキテクチャ，各チャネルの平均危険側故障時間（$MTTF_d$）及び平均診断範囲 DC_{avg} に依存する。

共通原因故障（CCF）も考慮することが望ましい（指針については，**附属書 F** 参照）。

ソフトウェアを含む SRP/CS に対しては，**4.6** の要求事項を適用する。

定量的データを利用できない又は使用しない場合（例えば，低複雑システム），関連する全てのパラメータは最悪ケースを選択することが望ましい。

SRP/CS の組合せ又は単一の SRP/CS は，一つの PL をもつ場合がある。異なる PL をもつ複数の PL の組合せは，**6.3** において考慮される。

PL_r＝a～PL_r＝c の用途の場合，障害を回避する方策は十分であり，より高いリスクの PL_r＝d～PL_r＝e の用途に対する SRP/CS の構造には，障害の回避，検出又は耐性のための方策を提供することができる。実用的な方策は，冗長，多様性（ダイバーシティ），監視を含む（**JIS B 9700-2** の **3.**及び **JIS B 9960-1** 参照）。

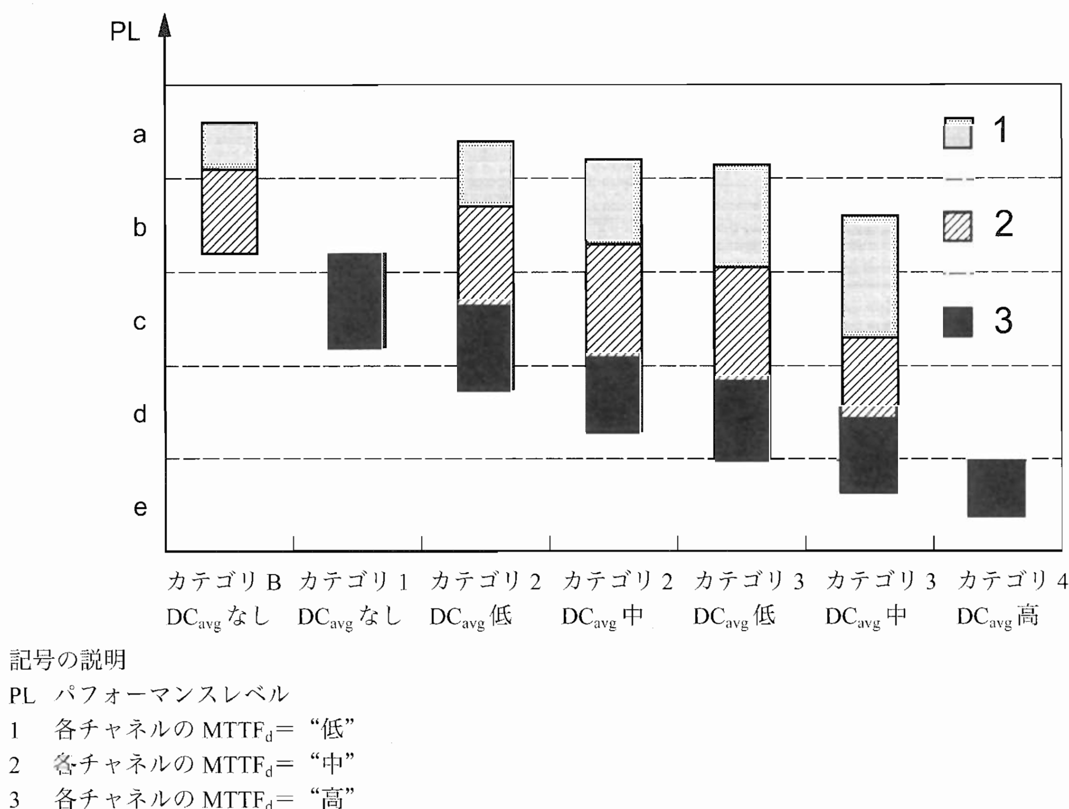
図 5 は，安全機能の要求 PL_r を達成するために，各チャネルの $MTTF_d$ 及び平均診断範囲 DC_{avg} と組み合わせたカテゴリ選択の手順を示す。

PL の見積りに対して，**図 5** は平均診断範囲 DC_{avg}（水平軸）をもつカテゴリと，各チャネルの $MTTF_d$（バー）とカテゴリの様々な組合せを示す。ダイアグラムのバーの部分は，要求 PL_r を達成するために選

択可能な各チャネルの3通りの$MTTF_d$の範囲（“低”，“中”，“高”）を表す。

図5（箇条**6**の指定アーキテクチャに基づく異なるマルコフモデルの結果を表す）の単純化したアプローチを使用する前に，DC_{avg}，及び各チャネルの$MTTF_d$だけでなく，SRP/CSのカテゴリも決定しなければならない（箇条**6**及び**附属書C**～**附属書E**参照）。

カテゴリ2，3及び4に対しては，共通原因故障（CCF）に対する十分な方策を実施しなければならない（指針については，**附属書F**参照）。これらのパラメータを考慮して，SRP/CSによって達成されるPLを決定するための図法を，**図5**は示している。カテゴリ（共通原因故障を含む。）と平均診断範囲DC_{avg}の組合せによって，**図5**でいずれのコラムを選択するかが決定される。各チャネルの$MTTF_d$によって，関連するコラムのうちの三つの色付き部分の一つを選択しなければならない。達成されるPLは，この部分の垂直方向の位置によって，垂直軸で読み取ることができる。もし，2又は3通りのPLが選択可能な場合，達成されるPLは，**表7**で示される。各チャネルの$MTTF_d$の正確な値によるPLのより正確な数値的選択については，**附属書K**参照。



記号の説明
PL　パフォーマンスレベル
1　各チャネルの$MTTF_d$＝“低”
2　各チャネルの$MTTF_d$＝“中”
3　各チャネルの$MTTF_d$＝“高”

図5－カテゴリ，DC_{avg}，各チャネルの$MTTF_d$とPLとの関係

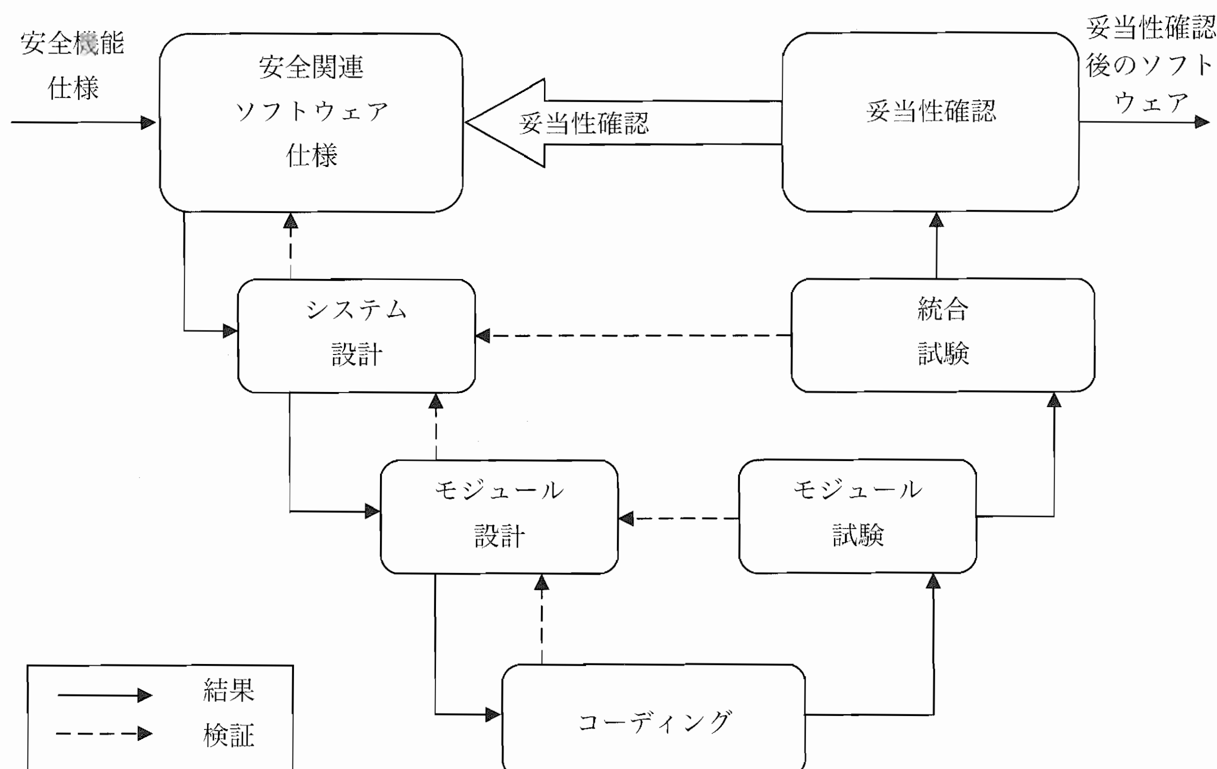
表 7－SRP/CS によって達成される PL を評価するための単純化手順

カテゴリ	B	1	2	2	3	3	4
DC_{avg}	“なし”	“なし”	“低”	“中”	“低”	“中”	“高”
各チャネルの $MTTF_d$							
“低”	a	該当なし	a	b	b	c	該当なし
“中”	b	該当なし	b	c	c	d	該当なし
“高”	該当なし	c	c	d	d	d	e

4.6 ソフトウェア安全要求事項

4.6.1 一般要求事項

安全関連の組込みソフトウェア又はアプリケーションソフトウェアの全ライフサイクル活動は，最初にソフトウェアライフサイクルの間に生じる障害の回避を考慮しなければならない（**図 6** 参照）。次の要求事項の主目的は，読取可能，理解可能，試験可能及び保守可能なソフトウェアとすることである。



注記 **附属書 J** に，ライフサイクル活動に対してより詳細な推奨事項を示す。

図 6－ソフトウェア安全ライフサイクルの単純化 V モデル

4.6.2 安全関連組込みソフトウェア（SRESW）

要求パフォーマンスレベル PL_r＝a～PL_r＝d までのコンポーネントの SRESW に対して，次の基本方策を適用しなければならない。

－ 検証及び妥当性確認活動を伴うソフトウェア安全ライフサイクル。**図 6** 参照。
－ 仕様及び設計の文書化
－ モジュール化及び構造化設計並びにコーディング
－ システマティック故障の抑制（**G.2** 参照）

－ ランダムハードウェア故障の抑制のためにソフトウェアによる方策を使用する場合，正確な実装の検証
－ 機能試験，例えば，ブラックボックス試験
－ 変更後の適切なソフトウェア安全ライフサイクル活動

要求パフォーマンスレベル PL_r＝c 又は PL_r＝d のコンポーネントの SRESW に対して，次の追加方策を適用しなければならない。

－ 例えば，**IEC 61508** 規格群又は **JIS Q 9001** と同等のプロジェクト管理及び品質管理システム
－ ソフトウェア安全ライフサイクルの間の全ての関連活動の文書化
－ 全ての構成品目を特定する構成管理及び SRESW の引渡しに関連した文書
－ 安全要求事項で構造化された仕様及び設計
－ 適切なプログラミング言語の使用，及び使用実績のあるコンピュータベースのツール
－ モジュール化及び構造化プログラミング，安全関連ではないソフトウェアとの分離，完全に定義されたインタフェースによって限定されたモジュールへの分割，標準設計及び標準コーディングの使用
－ 制御フロー解析におけるウォークスルー／レビューによるコーディングの検証
－ 拡張機能試験。例えば，グレイボックス試験，性能試験又はシミュレーション
－ 影響分析及び変更後の適切なソフトウェア安全ライフサイクル活動

要求パフォーマンスレベル PL_r＝e のコンポーネントの SRESW は，**IEC 61508-3** の箇条 **7** に適合し，SIL3 に適切に従うものとする。カテゴリ 3 又は 4 の SRP/CS で使用される 2 チャネルシステムでの仕様，設計，及びコーディングに多様性（ダイバーシティ）を使用するとき，要求パフォーマンスレベル PL_r＝e は，上述の要求パフォーマンスレベル PL_r＝c 又は PL_r＝d に対する方策を用いて達成することができる。

注記 1 これらの方策の詳細な記述については，例えば **IEC 61508-7** を参照。

注記 2 カテゴリ 3 又は 4 の SRP/CS で用いられるコンポーネントの設計及びコーディングにおいて多様性（ダイバーシティ）付き SRESW では，システマティック故障を避ける方策を施す上での努力は，例えば，コードの各行をチェックすることの代わりに構造面を考慮することだけによって，ソフトウェアの部分を再検討することで，システマティック故障を低減することができる。

4.6.3 安全関連アプリケーションソフトウェア（SRASW）

ソフトウェア安全ライフサイクル（**図 6** 参照）は，SRASW にも適用される（**附属書 J** 参照）。

制約可変言語（LVL）で記述され，次の要求事項に従う SRASW は，PL＝a～PL＝e を達成することができる。SRASW が無制約可変言語（FVL）で記述されている場合，SRESW に対する要求事項を適用しなければならず，それによってパフォーマンスレベル PL＝a～PL＝e までが達成可能となる。

一つのコンポーネント内の SRASW の一部が，異なるパフォーマンスレベル PL をもつ複数の安全機能に影響力（例えば，変更のため）をもつ場合，最も高いパフォーマンスレベル PL に関連する要求事項を適用しなければならない。

要求パフォーマンスレベル PL_r＝a～PL_r＝e までのコンポーネントの SRASW は，次の基本方策を適用しなければならない。

－ 検証及び妥当性確認での活動による安全ライフサイクルの開発，**図 6** 参照。
－ 仕様及び設計の文書化
－ モジュール化及び構造化プログラミング
－ 機能試験

－　変更後の適切な開発活動

要求パフォーマンスレベル PL_r＝c～PL_r＝e までのコンポーネントの SRASW に対して，効果向上（要求パフォーマンスレベル PL_r＝c の低効果，要求パフォーマンスレベル PL_r＝d の中効果，要求パフォーマンスレベル PL_r＝e の高効果）のために次の追加方策が必要とされる，又は推奨される。

a) 安全関連のソフトウェア仕様は，再検討されなければならず（**附属書 J** 参照），ライフサイクルに関わる全ての人が利用できるように作成され，次の記述を含まなければならない。

1) 要求 PL での安全機能及び関連する運転モード

2) 性能基準。例えば，反応時間

3) 外部信号インタフェースをもつハードウェアアーキテクチャ

4) 外部故障の検出及び抑制

b) ツール，ライブラリ，言語の選択

1) 使用上で信用を得た適切なツール

一つのコンポーネント及びそのツールで達成されたパフォーマンスレベル PL＝e に対して，ツールは適切な安全規格に適合しなければならない。多様なツールを用いて二つの多様なコンポーネントを使用する場合，使用上からの信用を十分とする必要がある。システマティックエラー（データ形不一致，曖昧なダイナミックメモリアロケーション，インタフェースの不完全な呼び出し，再帰，ポインタ演算など）を引き起こす原因となり得る状態を検出する技術的特徴が使用されなければならない。チェックは，実行中だけでなくコンパイル時にも実行されることが望ましい。ツールは，言語サブセット及びコーディングガイドライン，すなわち，少なくともスーパバイザ，又はそれらを使用する開発者のガイドで実施することが望ましい。

2) 妥当であって，かつ，実用的であるとき，妥当性が確認されたファンクションブロック（FB）ライブラリを使用することが望ましい。これには，ツールメーカによって提供される安全関連の FB ライブラリ（パフォーマンスレベル PL＝e のために特に推奨される），又は妥当性が確認されたアプリケーション特定の FB ライブラリで，かつ，この規格に適合するものが該当する。

3) モジュール化アプローチの正当な LVL サブセットを使用することが望ましい。例えば，許容された **JIS B 3503** 言語のサブセット。図式言語（例えば，ファンクションブロックダイアグラム，ラダー図）は，特に強く推奨される。

c) ソフトウェア設計は，次の特徴を備えなければならない。

1) データ及び制御フローを記述する半形式的な方法。例えば，状態図又はプログラムフローチャート

2) 妥当性確認された安全関連のファンクションブロックライブラリに由来するファンクションブロックによって主に実現されるモジュール化及び構造化プログラミング

3) コーディングが限定されたサイズのファンクションブロック

4) ファンクションブロックの中でのコードの実行は，一つの入力点及び一つの出力点をもつことが望ましい。

5) 入力⇒処理⇒出力における 3 ステージのアーキテクチャモデル（**図 7** 及び**附属書 J** 参照）

6) 一つのプログラム位置でのみの安全出力の割付け。

7) 外部故障の検出技術並びに入力，処理，及び安全状態につながる出力ブロックにおける防衛的なプログラミング技術の使用

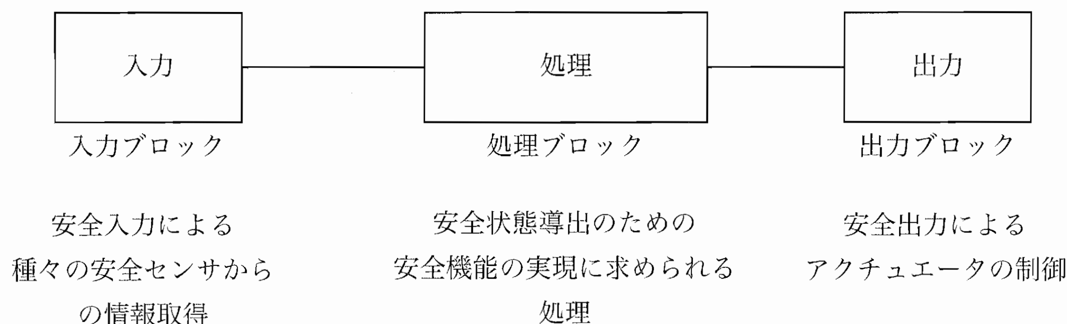


図 7－ソフトウェアの一般的なアーキテクチャモデル

d) 一つのコンポーネントでの SRASW 及び非 SRASW の結合

1) SRASW 及び非 SRASW は，明確に定義されたデータリンクにおいて異なるファンクションブロックでコード化されなければならない。

2) 安全関連の信号のインテグリティ（健全性）の低下に通じるような，安全関連及び非安全関連のデータの論理的結合があってはならない。このような結合の例には，安全関連及び非安全関連信号による論理的な“OR”による結合の結果が，安全関連信号を制御する場合などである。

e) ソフトウェアの実装／コーディング

1) コードは，読取可能，理解可能及び試験可能でなければならない。また，これらのために，明白なハードウェアアドレスに代わって，記号変数を使用することが望ましい。

2) 正当であるか，又は許容されたコーディングガイドラインを使用しなければならない。**附属書 J** 参照。

3) アプリケーション層（防衛的なプログラミング）で利用可能なデータのインテグリティ（健全性）及びプロウサビリティ（妥当性）のチェック（例えば，範囲チェック）を使用することが望ましい。

4) コードは，シミュレーションによって試験することが望ましい。

5) PL＝d 又は PL＝e の検証は，管理及びデータフロー分析によってなされることが望ましい。

f) 試験

1) 適切な妥当性確認の方法は，機能的な挙動及び性能基準（例えば，タイミング性能）に関するブラックボックス試験である。

2) PL＝d 又は PL＝e に対して，境界値解析によるテストケースの実行を推奨する。

3) 試験計画書の作成を推奨する。試験計画書には完成基準及び必要なツールを伴うテストケースを含めることが望ましい。

4) 入出力試験は，安全関連の信号が SRASW の中で正しく使用されることを保証しなければならない。

g) 文書化

1) 全てのライフサイクル及び変更活動は，文書化しなければならない。

2) 文書は，完全で，利用可能で，読込可能で，理解可能でなければならない。

3) ソーステキストの中のコード文書には，法人名，機能及び入出力の記述，バージョン及び使用されているファンクションブロックライブラリのバージョン，ネットワーク／命令文の十分なコメント，並びに宣言文の行を記述したモジュールヘッダを含まなければならない。

h) 検証

例　レビュー，検査，ウォークスルー，その他の適切な活動など。

注記 検証はアプリケーション特有のコードにだけ必要で，妥当性が確認されたライブラリ機能には必要ない。

i) 構成管理

特定の SRASW バージョンに関連する文書，ソフトウェアモジュール，検証・妥当性確認の結果及び特ツール構成を特定し，かつ，記録するために，その手順及びデータのバックアップをすることが望ましい。

j) 変更

SRASW の変更後に，仕様を保証するために影響分析を実施しなければならない。変更後に，適切なライフサイクル活動を実施しなければならない。変更のアクセス権を管理し，変更履歴を文書化しなければならない。

注記 変更は，既に使用中のシステムには影響を与えない。

4.6.4 ソフトウェアベースのパラメータ化

安全関連パラメータのソフトウェアベースのパラメータ化は，ソフトウェア安全要求仕様で記述されている SRP/CS 設計の安全関連の側面を考慮しなければならない。パラメータ化は，SRP/CS の供給者によって提供される専用ソフトウェアツールを用いて遂行しなければならない。このツールは，それ自身の識別（名前，バージョンなど）をもち，かつ，例えばパスワードの使用で権限のない変更を防止しなければならない。パラメータ化に使用される全てのデータのインテグリティ（健全性）を維持しなければならない。これは，次の方策を適用することによって達成しなければならない。

- 有効な入力範囲の抑制
- 伝送前のデータ破壊の抑制
- パラメータ伝送プロセスでのエラーによる影響の抑制
- 不完全なパラメータの伝送による影響の抑制
- パラメータ化に使用するツールのハードウェア／ソフトウェアの障害及び故障による影響の抑制

パラメータ化のツールは，この規格に従って SRP/CS のための全ての要求事項を満たさなければならない。又は，安全関連のパラメータを設定するために特別な手順を用いなければならない。この手順は，次のいずれかによって SRP/CS への入力パラメータの確認を含めなければならない。

- パラメータ化ツールへ変更されたパラメータの再伝送，又は
- パラメータのインテグリティ（健全性）を確認するための他の適切な手段

同様に，例えば，熟練した適切な人材による及びパラメータ化ツールでの自動的チェックの手段によるようなその後の確認も含めなければならない。

注記 1 パラメータ化がこの目的のために明確に意図されない装置（例えば，パーソナルコンピュータ又は同等物）を用いて実行される場合，これは特に重要である。

伝送／再伝送プロセスでの符号化／復号化のために用いられるソフトウェアモジュール及び，ユーザへの安全関連のパラメータの可視化のために用いられるソフトウェアモジュールは，最小限，システマティック故障を回避する機能（群）において多様性（ダイバーシティ）を用いなければならない。

ソフトウェアベースのパラメータ化の文書は，使用されるデータ（例えば，パラメータセットの事前定義）及び，SRP/CS に関連するパラメータ，パラメータ化を実施する人，パラメータ化の日付のような他の関連する情報とともに示さなければならない。

次の検証活動を，ソフトウェアベースのパラメータ化に対して適用しなければならない。

- それぞれの安全関連のパラメータ（最小，最大，代表値）に対する正しい設定の検証

- 安全関連のパラメータがプロウサビリティ（妥当性）についてチェックされることの検証。例えば，無効な値の使用など
- 安全関連パラメータの権限なしの変更防止の検証
- 障害が安全機能の喪失につながることが不可能な方法によるパラメータ化でのデータ／信号の生成及び処理の検証

 注記 2 パラメータ化がこの目的に対して明確に意図されない装置（例えば，パーソナルコンピュータ又は同等物）を用いて実行される場合，これは特に重要である。

4.7 達成した PL と要求 PL_r の適合検証

個々の安全機能に対して，安全関連 SRP/CS の PL は，**4.3** に従って決定される要求パフォーマンスレベル PL_r に適合しなければならない（**図 3** 参照）。これが満たされない場合，**図 3** に示されるプロセスを反復することが必要である。安全機能の一部となる異なる SRP/CS の PL は，その安全機能の要求パフォーマンスレベル PL_r と同等以上でなければならない。

4.8 人間工学的側面での設計

オペレータと SRP/CS との間のインタフェースは，合理的に予見可能な機械の誤使用を含めて，全ての意図する使用の間，人が危険にさらされないように設計し，実現しなければならない（**JIS B 9700-2**，**EN 614-1**，**ISO 9355-1**，**ISO 9355-2**，**ISO 9355-3**，**EN 1005-3**，**JIS B 9960-1** の箇条 **10**，**IEC 60447** 及び **JIS B 9706** 規格群参照）。

人間工学原則は，安全関連部を含めて機械及び制御システムを容易に使用し，かつ，オペレータが危険な方法で試行しないように利用しなければならない。

JIS B 9700-2 の **4.8** に示される人間工学原則の安全要求事項を適用する。

5 安全機能

5.1 安全機能仕様

この箇条は，SRP/CS によって提供できる安全機能のリスト及び詳細を規定する。設計者（又はタイプ C 規格作成者）は，特定の用途の制御システムで要請される安全方策を達成するために必要な安全機能を組み込まなければならない。

 例 安全関連停止機能，予期しない起動の防止，手動リセット機能，ミューティング機能，ホールド・ツゥ・ラン機能など。

 注記 機械の制御システムは，運転及び／又は安全の機能を提供する。運転機能（例えば，起動，通常停止）は，安全機能となり得るが，機械に関する十分なリスクアセスメントが実施された後だけ，これは確定させることができる。

表 8 及び**表 9** は，代表的な安全機能であり，その各々の特性及び安全関連パラメータをリスト化してあり，更に他の **JIS** 及び国際規格での安全機能に関する要求事項を参照している。設計者（又はタイプ C 規格作成者）は，**表 8** 及び**表 9** に掲げてある関連する安全機能に対して，全ての適用可能な要求事項を確実に満たさなければならない。

安全機能の特性によっては，追加の方策がこの箇条で述べられる。

必要な場合，特性及び安全機能の要求事項は，異なるエネルギー源を用いた使用に対して適用しなければならない。

表 8 及び**表 9** で参照される規格のほとんどが電気関連規格であるが，適用可能な要求事項は，他の技術方式の場合においても適用する必要がある。

表 8－典型的な機械の安全機能及びその特性に適用可能な JIS

安全機能／特性	要求事項			追加情報
	この規格	JIS B 9700-1	JIS B 9700-2	
安全防護物によって始動する安全関連停止機能 a)	5.2.1	3.26.8	4.11.3	JIS B 9960-1 の 9.2.2，9.2.5.3，9.2.5.5
手動リセット機能	5.2.2	－	－	JIS B 9960-1 の 9.2.5.3，9.2.5.4
起動／再起動機能	5.2.3	－	4.11.3，4.11.4	JIS B 9960-1 の 9.2.1，9.2.5.1，9.2.5.2，9.2.6
ローカル（局所）制御機能	5.2.4	－	4.11.8，4.11.10	JIS B 9960-1 の 10.1.5
ミューティング機能	5.2.5	－	－	－
ホールド・ツゥ・ラン機能	－	－	4.11.8 b)	JIS B 9960-1 の 9.2.6.1
イネーブル装置機能	－	－		JIS B 9960-1 の 9.2.6.3，10.9
予期しない起動の防止	－	－	4.11.4	JIS B 9714, JIS B 9960-1 の 5.4
捕捉された人の脱出及び救助	－	－	5.5.3	－
遮断及びエネルギの消散	－	－	5.5.4	JIS B 9714，JIS B 9960-1 の 5.3，6.3.1
制御モード及びモード選択	－	－	4.11.8，4.11.10	JIS B 9960-1 の 9.2.3，9.2.4
異なる制御システムの安全関連部間の相互作用	－	－	4.11.1 の最終文	JIS B 9960-1 の 9.3.4
安全関連入力値のパラメータ化の監視	4.6.4	－	－	－
非常停止機能 b)	－	－	5.5.2	JIS B 9703，JIS B 9960-1 の 9.2.5.4

注 a) インタロック付ガード及び制限装置（例えば，過速度，超過温度，超過圧力）を含む。
b) 付加保護方策については，JIS B 9700-1 参照。

表 9－安全機能及び安全関連パラメータの要求事項を示す国際規格及び JIS

安全機能／特性	要求事項		追加情報
	この規格	JIS B 9700-2	
応答時間	5.2.6	－	JIS B 9715 の 3.2，A.3，A.4
速度，温度又は圧力のような安全関連パラメータ	5.2.7	4.11.8 e)	JIS B 9960-1 の 7.1，9.3.2，9.3.4
電源の変動，喪失，復旧	5.2.8	4.11.8 e)	JIS B 9960-1 の 4.3，7.1，7.5
指示及び警告	－	4.8	ISO 7731 ISO 11428 ISO 11429 JIS B 9706-1 JIS B 9960-1 の 10.3，10.4 IEC 61131 規格群 JIS B 9961

安全機能を同定し，かつ，指定する場合，少なくとも次を考慮しなければならない。

a) 個々の危険源又は危険状態に対するリスクアセスメントの結果

b) 次を含む，機械の運転特性

－ 機械の意図する使用（合理的に予見可能な誤使用を含む。）

－ 運転モード［例えば，ローカル（局所）モード，自動モード，機械の一区域又は一部分に関連するモード］

－ サイクルタイム
－ 応答時間

c) 非常操作

d) 異なる作業プロセス及び手動作業（修理，調整，清掃，トラブルシューティングなど）での相互作用に関する記述

e) 安全機能で達成する又は回避する機械の挙動

f) 機械が作動可能又は不可能となる条件（運転モードなど）

g) 運転頻度

h) ある機能が同時に作動した場合の優先順位

5.2 安全機能の詳細

5.2.1 安全関連停止機能

表 8 の要求事項に加えて，次を適用する。

安全関連停止機能（例えば，安全防護物によって始動する）は，作動後必要に応じて速やかに機械を安全状態に移行しなければならない。このような停止は，通常運転の停止に対し，優先的でなければならない。

一連の機械がある統制下でともに動作する場合，上述の停止条件にあることを管理制御及び／又はその他の機械に対して信号で伝えるための処置を講じなければならない。

注記 安全関連停止機能は，運転上で問題を生じる場合があり，また，例えばアーク溶接作業では再起動が困難になる場合が起こる。

安全関連停止機能の無効化の試みを低減するために，実際の運転を完了させるための中止操作を先行させ，また停止位置から容易で，かつ，迅速な再起動手段を準備することがある（例えば，生産に対する損害を与えることなく）。

この一つの解決法は，サイクルが容易な再起動を可能にする規定の位置に到達した場合，ガード施錠が開放されるような施錠式インタロック装置の使用である。

5.2.2 手動リセット機能

表 8 の要求事項に加えて，次を適用する。

停止命令が安全防護物によって始動した後，再起動のための安全条件が存在するまで，その停止条件を維持しなければならない。

安全防護物をリセットすることによって安全機能を再設定することは，停止命令を消去することである。リスクアセスメントによって示される場合，この停止命令の消去は，手動で，独立して，かつ，故意の動作（手動リセット）で確認されなければならない。

手動リセットの機能は，次でなければならない。

－ SRP/CS 内で個別に，かつ，手動で操作される装置を介して提供される。
－ 全ての安全機能及び安全防護物が動作可能であるときだけ実行される。
－ リセット自体で機械の始動又は危険状態の始まりを生じない。
－ 故意の動作による。
－ 個別の起動命令を受け入れるための制御システムを備える。
－ アクチュエータの励起（オン）位置からの開放動作だけを受け入れる。

手動リセット機能を備える SRP/CS のパフォーマンスレベルは，手動リセット機能を備えることによって関連の安全機能で要求される安全性を低下させないように選択しなければならない。

リセットアクチュエータは，危険区域の外で，危険区域内の人の不在を目視によってチェックしやすいような安全な位置に配置しなければならない。

危険区域の視認性が完全でない場合，特別のリセット手順が要求される

注記 一つの解決策は，第 2 のリセットアクチュエータの使用である。リセット機能は，危険区域の外側（安全防護物の近くで）に配置した第 2 のリセットアクチュエータと組み合わせて，第 1 のアクチュエータによって危険区域内で始動する。このリセットの手順は，制御システムが別の起動命令を受け取る前の制限時間内で実現することが必要である。

5.2.3　起動／再起動機能

表 8 の要求事項に加えて，次を適用する。

再起動は危険状態が存在しない場合にだけ自動的に行われなければならない。特に起動機能付のインタロック付ガードに関しては，**JIS B 9700-2** の **5.3.2.5** を適用する。

起動及び再起動に対するこれらの要求事項は，遠隔制御が可能な機械にも適用しなければならない。

注記 制御システムへのセンサからのフィードバック信号は，自動的な再起動を始動することができる。

例 機械の自動運転では，制御システムへのセンサのフィードバック信号は，プロセスフローを制御するために，しばしば使用される。加工物が加工位置からずれた場合，プロセスフローは停止する。インタロック付きの安全防護物の監視が自動的プロセス制御に優先しない場合，オペレータが加工物を再調整する間，機械を再起動する危険が生じる可能性がある。したがって，遠隔制御による再起動は，安全防護物が再び閉じて，保全員が危険区域を離れるまで，許可されてはならない。制御システムによる予期しない起動の防止への寄与度は，リスクアセスメントの結果に依存する。

5.2.4　ローカル（局所）制御機能

表 8 の要求事項に加えて，次を適用する。

機械が，例えば，携行式制御装置又はペンダントによってローカルに（局所で）制御される場合，次を適用しなければならない。

－ ローカル制御を選択するための手段は，危険区域外に配置しなければならない。
－ リスクアセスメントで定めた区域におけるローカル制御器によってだけ，危険条件を始動可能としなければならない。
－ ローカル（局所）制御と主制御間の切替えで，危険状態を生じてはならない。

5.2.5　ミューティング機能

表 8 の要求事項に加えて，次を適用する。

ミューティングによっていかなる人も危険状態にさらされることがあってはならない。ミューティング中は，他の手段によって安全条件が提供されなければならない。

ミューティングの終了では SRP/CS の全ての安全機能が復旧しなければならない。

ミューティング機能を備える安全関連部のパフォーマンスレベルは，ミューティング機能を含むことによって，関連する安全機能で要求される安全性を損なうことがないように選択しなければならない。

注記 用途によっては，ミューティングの表示信号を必要とする。

5.2.6　応答時間

表 9 の要求事項に加えて，次を適用する。

リスクアセスメントで要請される場合，SRP／CS の応答時間を決定しなければならない（箇条 **11** 参照）。

注記　制御システムの応答時間は，その機械全体の応答時間の一部である。その機械で必要な全体の応答時間は，安全関連部の設計，例えばブレーキシステムを備えることの必要性，に影響することになる。

5.2.7　安全関連パラメータ

表 9 の要求事項に加えて，次を適用する。

安全関連パラメータ，例えば，位置，速度，温度，又は圧力が現在の制限から逸脱する場合，制御システムは適切な方策，例えば停止動作，警告信号，アラームを始動させなければならない。

プログラマブル電子システムの安全関連データに関する手動入力エラーによって危険状態を生じるおそれがある場合，安全関連制御システム内に，例えば限界，フォーマット及び／又は論理的入力値に関するチェックシステムのようなデータチェックシステムを備えなければならない。

5.2.8　動力源の変動，喪失及び復旧

表 9 の要求事項に加えて，次を適用する。

エネルギ供給の喪失を含めて，設計上の動作範囲外のエネルギレベルの変動が生じた場合，SRP/CS は，機械システムの他の部分において安全状態を維持できるように出力信号を生成し続ける，又は始動させなければならない。

6　カテゴリと各チャネルの $MTTF_d$，DC_{avg} 及び CCF の関係

6.1　一般要求事項

SRP/CS は，**6.2** で規定される 5 通りのカテゴリのうち，一つ以上のカテゴリの要求事項に従っていなければならない。カテゴリは，特定の PL を達成するために使用される基本的なパラメータである。箇条 **4** に記述される設計上での考慮事項に基づく障害に対する抵抗性に関して，SRP/CS に要求される挙動を述べている。

カテゴリ B は，基本カテゴリである。障害の発生は，安全機能の喪失につながる。カテゴリ 1 では，障害に対する抵抗性の向上は主としてコンポーネントの選択及び適用によって達成される。カテゴリ 2，3，4 では，指定される安全機能に関するパフォーマンスの向上は，主として SRP/CS の構造の改良によって達成できる。カテゴリ 2 では，指定される安全機能が働くことを定期的にチェックすることによって実現できる。

カテゴリ 3，4 では，単一障害が安全機能の喪失を招かないことを確実にすることによって実現できる。カテゴリ 4 の場合，及びカテゴリ 3 で合理的に実施可能な場合は常に，その単一障害は検出できるようにする。カテゴリ 4 では，障害の蓄積に対する抵抗性が規定される。

表 10 は，SRP/CS のカテゴリの概要，要求事項及び障害が発生した場合のそのシステムの挙動を示す。

コンポーネントの故障の原因を考える場合，障害によってはそれを除外することが可能である（箇条 **7** 参照）。

個々の SRP/CS でのカテゴリの選択は，主に次に依存する。

－　安全関連部が寄与する安全機能によって達成されるリスクの低減
－　要求パフォーマンスレベル PL_r
－　使用される技術
－　SRP/CS での障害発生時におけるリスク
－　SRP/CS での障害回避の可能性（システマティック障害）
－　SRP/CS のある部分及び障害の発生確率及び関連パラメータ

－ 平均危険側故障時間（$MTTF_d$）
－ 診断範囲（DC）
－ カテゴリ 2，3 及び 4 の場合における共通原因故障（CCF）

6.2 カテゴリの仕様

6.2.1 一般要求事項

各 SRP/CS は，関連するカテゴリの要求事項に適合しなければならない（**6.2.3**～**6.2.7** 参照）。

6.2.3～**6.2.7** の典型的なアーキテクチャは，各カテゴリの要求事項を満たす。

図 8～**図 12** は，例ではなく一般的なアーキテクチャを示す。このアーキテクチャからの逸脱は常に可能である。しかし，いずれの逸脱も，適切な分析ツール（例えば，マルコフモデル，FTA）の手段によって正当化し，かつ，システムは要求パフォーマンスレベル PL_r を満たさなければならない。

指定アーキテクチャは，回路図としてだけでなく，論理図としても考慮することができる。カテゴリ 3 及び 4 に対しては，全ての部分が必ずしも物理的に冗長系であるということではなく，一つの障害が安全機能を喪失しないということを確実にするために冗長手段があるということを，これは意味している。

図 8～**図 12** までの線及び矢印は，論理的な相互接続の手段及び論理的に可能な診断手段を示している。

6.2.2 指定アーキテクチャ

SRP/CS の構造は，PL に大きな影響を及ぼすキーとなる特性である。構造の種類が多様であっても，基本構成は，しばしば類似のものとなる。このように，機械分野において存在するほとんどの構造は，カテゴリのうちの一つに割り当てることができる。各カテゴリに対しては，安全関連ブロックダイアグラムとして典型的な代表図を示すことができる。典型的な図は，指定アーキテクチャと呼ばれ，次の各カテゴリの要求事項のなかでリスト化して示される（**図 8**～**図 12** 参照）。

重要なことは，**図 5** で示される PL は，カテゴリ，各チャネルの $MTTF_d$ 及び DC_{avg} によって，指定アーキテクチャに基づいているということである。**図 5** が PL を見積るために使用される場合，SRP/CS のアーキテクチャは，主張されるカテゴリの指定アーキテクチャと同等であるということを立証することが望ましい。一般的に，各カテゴリの特性を満たす設計は，カテゴリの各指定アーキテクチャと同等である。

注記 個々の技術的解決策から生じるか，又はタイプ C 規格によって決定される場合，SRP/CS の安全関連のパフォーマンスは，PL_r の追加要求なしにカテゴリによってだけ要求される場合がある。このような場合，安全性は特にアーキテクチャによって提供されることとなり，MTTF，DC 及び CCF の要求事項は，適用しない。

6.2.3 カテゴリ B

制御システムの安全関連部は，最小限，関連規格に従い，かつ，次の事項に対して抵抗性をもてるように特定の用途のための基本安全原則を用いて，設計，製造，選択，組立及び結合されなければならない。

－ 予想される操作のストレス，例えば，遮断容量及び頻度に関する信頼性
－ 加工材料の影響，例えば，洗浄機の洗剤
－ 他の関連する外部影響，例えば，機械的振動，電磁干渉，動力供給の中断又は妨害

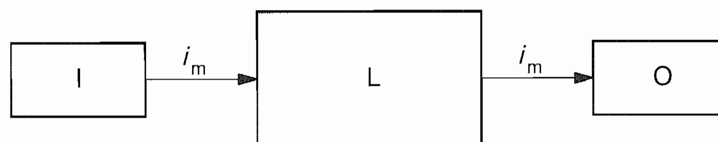
カテゴリ B のシステム内では診断範囲がなく（DC_{avg}＝0 %），かつ，各チャネルの $MTTF_d$ は，“低”～“中”までとなる。そのような構造（通常，単一チャネルシステム）においては，共通原因故障への考慮は不要である。

カテゴリ B によって達成可能な最大 PL は，PL＝b である。

注記 一つの障害の発生が，安全機能の喪失につながり得る。

電磁両立性の特定の要求事項は，例えば，パワードライブシステムの規格 **JIS C 4421** の関連製品規格で

規定される。SRP/CS の機能安全に対しては，特に，イミュニティが関連する。製品規格が存在しない場合，少なくとも，**JIS C 61000-6-2** のイミュニティの要求事項に従うことが望ましい。



記号の説明
i_m　相互接続手段
I　入力装置，例えば，センサ
L　論理
O　出力装置，例えば，主接触器

図 8－カテゴリ B の指定アーキテクチャ

6.2.4　カテゴリ 1

カテゴリ 1 に対しては，**6.2.3** のカテゴリ B の要求事項を適用しなければならない。また，追加して次を適用する。

カテゴリ 1 の SRP/CS は，“十分吟味された”コンポーネント及び“十分吟味された”安全原則を用いて設計及び製作しなければならない（**ISO 13849-2** 参照）。

安全関連への適用のために“十分吟味された”コンポーネントは，次のいずれかのコンポーネントである。

a) 類似のアプリケーションにおいて好結果で過去に広く使用された。

b) 安全関連へのアプリケーションに対して適切性及び信頼性を論証するための原則を用いて製作され，かつ，検証された。

新しく開発されたコンポーネント及び安全原則は，**b)**の条件を満たす場合，“十分吟味された”に同等と考えてよい。

個々のコンポーネントが“十分吟味された”と容認する決定は，アプリケーションに依存する。

注記 1　複雑な電子式コンポーネント（例えば，PLC，マイクロプロセッサ，ASIC（特定用途向け集積回路）は，“十分吟味された”と同等と考えることはできない。

各チャネルの $MTTF_d$ は，“高”でなければならない。

カテゴリ 1 によって達成可能な最大 PL は，PL＝c である。

注記 2　カテゴリ 1 のシステム内には診断範囲はなく（DC_{avg}＝0 %），そのような構造（単一チャネルシステム）においては，共通原因故障（CCF）への考慮は不要である。

注記 3　一つの障害発生時，安全機能の喪失につながり得る。しかし，カテゴリ 1 における各チャネルの $MTTF_d$ は，カテゴリ B よりも長く，結果として，安全機能の喪失はより少ない。

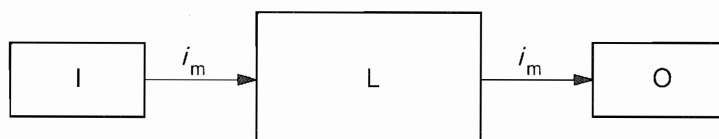
“十分吟味された”コンポーネントと“障害の除外”（箇条 **7** 参照）との間を明確に区別することが重要ある。

コンポーネントに対する“十分吟味された”としての能力は，そのアプリケーションに依存する。例えば，ポジティブオープンの接点を備えた位置スイッチは，工作機械にとって“十分吟味された”と考慮され得るが，食品産業におけるアプリケーションには不適切となる。例えば，乳製品産業において，このスイッチは，数箇月後に乳酸によって破壊されることになる。

障害の除外は，非常に高い PL につながり得るが，この障害の除外を許すために採られる適切な方策は，

装置の全寿命の間で適用されることが望ましい。これを確実にするために，制御システム外の追加方策を必要とすることがある。位置スイッチの場合，この種の方策の例は，次のとおりである。

－　調整後にスイッチの固定を確実にするための手段
－　カムの固定を確実にするための手段
－　カムの方向の安定性を確実にするための手段
－　位置スイッチのオーバトラベル回避のための手段。例えば，衝撃吸収装置及び調整装置の固定強度
－　外部からの損傷に対して保護するための手段



記号の説明
i_m　相互接続手段
I　入力装置，例えば，センサ
L　論理
O　出力装置，例えば，主接触器

図 9－カテゴリ 1 の指定アーキテクチャ

6.2.5　カテゴリ 2

カテゴリ 2 に対しては，**6.2.3** のカテゴリ B の要求事項を適用しなければならない。また，**6.2.4** の“十分吟味された安全原則”にも従わなければならない。さらに追加して，次を適用する。

カテゴリ 2 の SRP/CS は，その機能を機械制御システムによって，適切な間隔でチェックするように設計しなければならない。安全機能のチェックは，次で遂行しなければならない。

－　機械の起動時，及び
－　危険状態の始まる前，例えば，新たなサイクルの起動，他の動きの起動，及び／又はリスクアセスメント及び運転の種類によって必要とする場合で，運転中，定期的に。

このチェックの始動は，自動的である場合がある。安全機能の全てのチェックは，次のいずれかでなければならない。

－　障害が検出されない場合には，運転を許可する。又は
－　障害が検出された場合には，適切な制御動作を始動するために出力信号を発生する。

可能である場合，この出力は安全状態を始動しなければならない。障害が除去されるまで，安全状態を維持しなければならない。安全状態を始動することが不可能である場合（例えば，最終開閉器における接点の溶着），出力は危険を警告しなければならない。

カテゴリ 2 の指定アーキテクチャでは，**図 10** で示すように，$MTTF_d$ 及び DC_{avg} の計算は，機能的チャネルのブロック（例えば，**図 10** の I，L 及び O）だけを考慮し，試験チャネルのブロック（例えば，**図 10** の TE 及び OTE）は考慮しないほうがよい。

障害検出を含む全 SRP/CS の診断範囲（DC_{avg}）は，“低”又は“中”でなければならない。各チャネルの $MTTF_d$ は，要求パフォーマンスレベル PL_r によって，“低”～“高”まででなければならない。CCF に対する方策を適用しなければならない（**附属書 F** 参照）。

チェック自体が危険状態につながってはならない（例えば，応答時間の増加による）。チェックの装置は，安全機能を提供する安全関連部に統合される，又は分離される場合がある。

カテゴリ 2 によって達成可能な最大 PL は，PL＝d である。

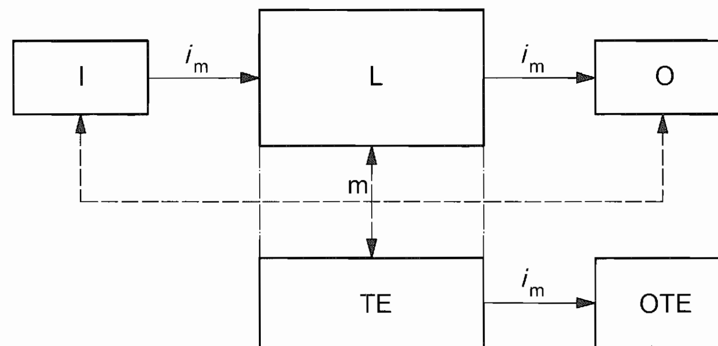
注記 1 安全機能のチェックが全てのコンポーネントに適用できないために，カテゴリ 2 を使用できない場合がある。

注記 2 カテゴリ 2 のシステムには，次の挙動が許される。

－ チェック間での障害の発生が安全機能の喪失につながり得る。

－ 安全機能の喪失は，チェックによって検出される。

注記 3 カテゴリ 2 の機能の妥当性を支援するための原則は，採用の技術規定，及び，例えばチェック頻度の選択によって危険状態の発生確率を低減させ得ることに基づく。



破線は，合理的に実行可能な障害検出を表す。

記号の説明

i_m 相互接続手段
I 入力装置。例えば，センサ
L 論理
m 監視
O 出力装置。例えば，主接触器
TE 試験装置
OTE 試験装置の出力

図 10－カテゴリ 2 の指定アーキテクチャ

6.2.6 カテゴリ 3

カテゴリ 3 に対しては，**6.2.3** のカテゴリ B に準じた同様の要求事項を適用しなければならない。また，**6.2.4** に従って“十分吟味された安全原則”にも従わなければならない。さらに加えて，次を適用する。

カテゴリ 3 の SRP/CS は，そのいずれの部分に単一障害が生じても，それが安全機能の喪失につながらないように設計しなければならない。合理的に実施可能な場合はいつでも，単一障害は，安全機能の次の動作要求時，又はそれ以前に検出されなければならない。

障害検出を含む全 SRP/CS の診断範囲（DC_{avg}）は，“低”又は“中”でなければならない。冗長チャネルの各々の $MTTF_d$ は，PL_r によって，“低”～“高”まででなければならない。CCF に対する方策を適用しなければならない（**附属書 F** 参照）。

注記 1 単一障害検出の要求事項は，全ての障害が検出されることを意味しない。結果として，未検出の障害が蓄積し，機械的に意図しない信号の出力及び危険状態につながる場合がある。障害検出に対して実施可能な方策の代表的な例は，機械的にガイドされるリレー接点のフィードバック及び冗長な電気的出力の監視への使用である。

注記 2 C タイプの規格作成者は，障害検出に関して，それが技術方式及び適用上の理由で必要とさ

れる場合，更に詳細を示す必要がある。

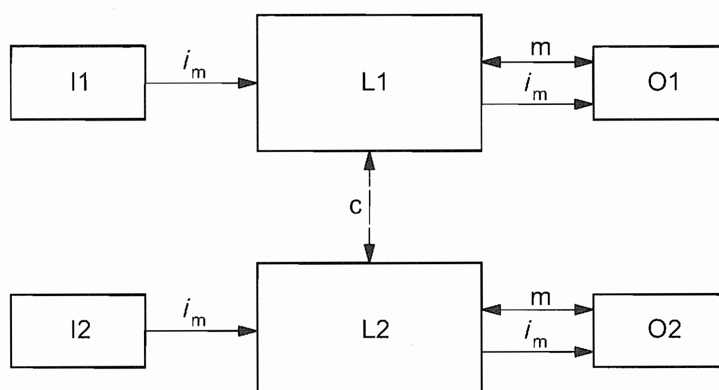
注記 3　カテゴリ 3 のシステムには，次の挙動を許す。

－　単一障害発生時，安全機能が常に遂行される。

－　全てではないが，障害によっては検出される。

－　未検出の障害の蓄積が，安全機能の喪失につながり得る。

注記 4　使用される技術方式が，障害検出の実施の可能性に影響する場合がある。



監視を示す線は，合理的に実行可能な障害検出を示す。

記号の説明

i_m　相互接続手段

c　相互監視

I1，I2　入力装置。例えば，センサ

L1，L2　論理処理

m　監視

O1，O2　出力装置。例えば，主接触器

図 11－カテゴリ 3 の指定アーキテクチャ

6.2.7　カテゴリ 4

カテゴリ 4 に対しては，**6.2.3** のカテゴリ B に準じた同様の要求事項を適用しなければならない。また，**6.2.4** の“十分吟味された安全原則”にも従わなければならない。さらに加えて，次を適用する。

カテゴリ 4 の SRP/CS は，次のように設計しなければならない。

－　安全関連部のいずれにおいても単一障害は，安全機能の喪失につながらない。かつ，

－　その単一障害は，安全機能の次の動作要求時，又はそれ以前であって，例えば，直ちに，始動時，又は機械の運転サイクルの終了時に検出される。

しかし，この検出が不可能な場合，未検出障害の蓄積が安全機能の喪失につながってはならない。

全 SRP/CS の診断範囲（DC_{avg}）は，障害の蓄積を含めて，“高”でなければならない。冗長チャネルの各々の $MTTF_d$ は，“高”でなければならない。CCF に対する方策を適用しなければならない（**附属書 F** 参照）。

注記 1　カテゴリ 4 のシステムには，次の挙動が許される。

－　単一障害発生時，安全機能が常に働く。

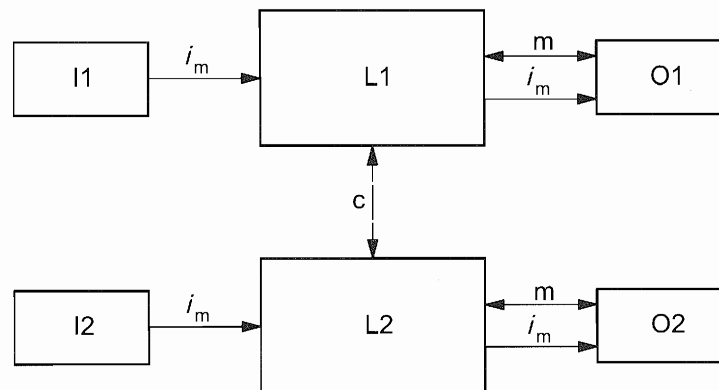
－　障害は，安全機能の喪失を防止するために，適時検出される。

－　未検出障害の蓄積を考慮する。

注記 2　カテゴリ 3 及びカテゴリ 4 の相違は，カテゴリ 4 では DC_{avg} が“高”で，かつ，各チャネル

に要求される $MTTF_d$ は，“高”だけである。

実用的には，二つの障害の組合せとなる障害の考慮だけで十分とする場合がある。



監視を示す線は，カテゴリ 3 の指定アーキテクチャよりも高い診断範囲を表す。

記号の説明

i_m　相互接続手段

c　相互監視

I1，I2　入力装置。例えば，センサ

L1，L2　論理処理

m　監視

O1，O2　出力装置。例えば，主接触器

図 12－カテゴリ 4 の指定アーキテクチャ

表 10－カテゴリ要求事項の要約

カテゴリ	要求事項要約	システム挙動	安全性達成のために使用される原則	各チャネルの $MTTF_d$	DCavg	CCF
B (**6.2.3** 参照)	コンポーネントのみならずSRP/CS 及び／又は保護装置は，予想される影響に耐えるように，関連規格に従って設計，製造，選択，組立，組み合わされること。基本安全原則を用いること。	障害発生時，安全機能の喪失を招くことがある。	主としてコンポーネントの選択によって特徴づけられる。	“低”～“中”	“なし”	関連なし
1 (**6.2.4** 参照)	B の要求事項が適用されること。“十分吟味された”コンポーネント及び“十分吟味された”安全原則を用いること。	障害発生時，安全機能の喪失を招くことがあるが，発生する確率はカテゴリ B より低い。	主としてコンポーネントの選択によって特徴づけられる。	“高”	“なし”	関連なし
2 (**6.2.5** 参照)	B の要求事項及び“十分吟味された”安全原則の使用が適用されること。安全機能は機械の制御システムによって適切な間隔でチェックされること。	チェック間の障害の発生が安全機能の喪失を招くことがある。 安全機能の喪失はチェックによって検出される。	主として構造によって特徴づけられる。	“低”～“高”	“低”～“中”	**附属書 F** 参照
3 (**6.2.6** 参照)	B の要求事項及び“十分吟味された”安全原則の使用が適用されること。安全関連部は次のように設計されていること。 － いずれの部分の単一障害も安全機能の喪失を招かない。かつ， － 合理的に実施可能な場合は常に単一障害が検出される。	単一障害発生時，安全機能が常に機能する。 全てではないが障害の幾つかは検出される。 検出されない障害の蓄積で安全機能の喪失を招くことがある。	主として構造によって特徴づけられる。	“低”～“高”	“低”～“中”	**附属書 F** 参照
4 (**6.2.7** 参照)	B の要求事項及び“十分吟味された”安全原則の使用が適用されること。 安全関連部は次のように設計されること。 － いずれの部分の単一の障害も安全機能の喪失を招かない。かつ， － 単一障害は，安全機能に対する次の動作要求のとき，又はそれ以前に検出される。それが不可能な場合，障害の蓄積が安全機能の喪失を招かないこと。	障害発生時，安全機能が常に機能する。 蓄積された障害の検出によって，安全機能の喪失の可能性が低減する（高 DC）。 障害は安全機能の喪失を防止するために適時検出される。	主として構造によって特徴づけられる。	“高”	“高” （障害の蓄積を含む。）	**附属書 F** 参照
注記　完全な要求事項は，箇条 **6** 参照。						

6.3　総合的な PL を達成するための SRP/CS の組合せ

安全機能は，複数の SRP/CS の組合せ，すなわち，入力システム，信号処理ユニット，出力システムによって実現可能である。この場合の SRP/CS は一つ及び／又は異なるカテゴリに割り当てられる場合がある。使用される SRP/CS の各々に対して，**6.2** によるカテゴリを選択しなければならない。この SRP/CS の

組合せに対しては，総合的な PL を**表 11** を使用して特定しなければならない。この場合，SRP/CS の組合せの妥当性確認が要求される（**図 3** 参照）。

6.2 に従って組み合わされた制御システムの安全関連部は，安全関連信号で始まって，かつ，動力制御要素の出力で終了する点を用いて起動する。しかし，組合せの SRP/CS は，線形（直列配置）又は冗長（並列配置）の方法で接続される複数の部分で構成される場合がある。組合せの SRP／CS によるパフォーマンスレベル PL の新たな見積りの複雑性を回避するために，全ての部分の個々の PL が既に計算されている場合での，SRP/CS の直列配置に対する見積りは次による。

全安全機能の遂行の全体として，直列配置で N 個の分離された SRP/CS_i を仮定する。各 SRP/CS_i に対して，PL_i は既に見積り済みである。この状況は**図 13** で示してある（**図 4** 及び**図 H.2** 参照）。

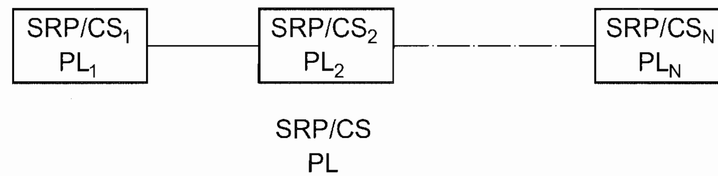


図 13－総合的な PL を達成するための SRP/CS の組合せ

次の方法によって，安全機能を遂行する組合せ全体の SRP/CS の PL を計算できる。

a) 最も低い PL_i を定めて，それを PL_{low} とする。

b) $PL_i = PL_{low}$ とする SRP/CS_i の個数 N_{low} を特定する。

c) PL は**表 11** を参照して定める。

表 11－SRP/CS を直列に配置した場合の PL の計算

PL_{low}	N_{low}	⇒	PL
a	＞3	⇒	“なし”，許可されない
	≦3	⇒	a
b	＞2	⇒	a
	≦2	⇒	b
c	＞2	⇒	b
	≦2	⇒	c
d	＞3	⇒	c
	≦3	⇒	d
e	＞3	⇒	d
	≦3	⇒	e
注記　この参照表で算定される値は，各 PL の中間点の信頼性データに基づく。			

7　障害の考慮，障害の除外

7.1　一般要求事項

選択のカテゴリに従って，要求パフォーマンスレベル PL_r を達成するように，安全関連部を設計し，耐障害の能力を査定しなければならない。

7.2　障害の考慮

種々の技術方式での重要な故障及び障害のリストは，**ISO 13849-2** で示される。障害リストは，必ずしも除外を意味するのではなく，必要な場合，追加の障害を考慮し，掲載しなければならない。このような場合，評価方法もまた明瞭に作成することが望ましい。**ISO 13849-2** で示されない新しいコンポーネント

に対しては，考慮する障害を設定して FMEA（**IEC 60812** 参照）を実施しなければならない。

一般的に，次の障害基準を考慮しなければならない。

－ 障害の結果として，更にコンポーネントに障害が生じる場合，続く全ての障害を一緒にして最初の障害は，単一障害として考慮しなければならない。
－ 共通の原因による二つ以上の個別の障害は，単一障害として見なされなければならない（これは，CCF として知られている)。
－ 個別の原因で生じる二つ以上の障害の同時発生は，著しく見込みがなく，従って考慮の必要はない。

7.3 障害の除外

ある程度の障害の除外を仮定しないで，SRP/CS を評価することは必ずしも可能ではない。障害の除外に関する詳細な情報は，**ISO 13849-2** 参照。

障害の除外は，技術的な安全の要求事項と，障害の発生の理論的可能性との間の妥協である。

障害の除外は，次による。

－ 幾つかの障害発生の技術的な非現実性
－ 考慮した用途に独立して，一般的に受け入れられる技術的経験，及び
－ 用途及び特定の危険源に関連した技術的要求事項

障害を除外する場合，技術文書により詳細な理由を示さなければならない。

8 妥当性確認

SRP/CS の設計では，妥当性確認を実施しなければならない（**図 3** 参照)。妥当性確認は，各安全機能を提供する SRP/CS の組合せが，この規格に関する全ての要求事項を満たすということを立証しなければならない。

妥当性確認の詳細に対しては，**ISO 13849-2** 参照。

9 保全

予防又は是正の保全は，安全関連部の特定の性能を維持するために必要である。時間の経過とともに指定の性能からの逸脱は，安全性の低下，又は危険状態にもなり得る。SRP/CS の使用上の情報には，SRP/CS の保全指示書を含めなければならない（定期検査を含む。)。

制御システムの安全関連部の保全性に関する規定は，**JIS B 9700-2** の **4.7** に示す原則に従わなければならない。保全に関する全ての情報は，**JIS B 9700-2** の **6.5.1 e)**に適合しなければならない。

10 技術文書

SRP/CS を設計する場合，設計者は，少なくとも SRP/CS に関連する次の情報を文書化しなければならない。

－ SRP/CS によって提供される安全機能
－ 各安全機能の特性
－ 安全関連部の正確な起点及び終了点
－ 環境条件
－ パフォーマンスレベル PL
－ 選択したカテゴリ又は複数の場合，各カテゴリ
－ 信頼性に関連するパラメータ（$MTTF_d$，DC，CCF 及び使命時間）

－　システマティック故障に対する方策
－　使用した技術方式又は複数の場合，各技術方式
－　考慮した全ての安全関連障害
－　障害の除外に関する正当化の根拠（**ISO 13849-2** 参照）
－　設計の論理的根拠（例えば，考慮した障害，除外した障害）
－　ソフトウェア関連文書
－　合理的に予見可能な誤使用に対する方策

注記　一般的に，文書類は，製造業者内部での使用を目的としており，機械の使用者には配布されないと予見される。

11　使用上の情報

JIS B 9700-2 の **6.5.2** の原則及び他の関連文書（例えば，**JIS B 9960-1** の箇条 **17**）の適用可能な箇条を適用しなければならない。特に，SRP/CS の安全な使用に際しての重要な情報は，使用者に示されなければならない。これは次を含むが，この限りではない。

－　選定したカテゴリに対する安全関連部の制限及び障害の除外の全て
－　SRP/CS の制限及び障害除外の全て（**7.3** 参照）。選定したカテゴリ（又は複数のカテゴリ）及び安全性能の維持のために必須である場合，その障害の除外を継続的に正当化するために，適切な情報（例えば，修正，保全及び修理対応）を示すことが望ましい。
－　安全機能における指定性能からの逸脱の影響
－　SRP/CS 及び保護装置へのインタフェースの明瞭な記述
－　応答時間
－　運転制限（環境条件を含む。）
－　指示及び警告
－　安全機能のミューティング及び中断
－　制御モード
－　保全（箇条 **9** 参照）
－　保全チェックリスト
－　内部部品へのアクセス及び交換の容易性
－　容易かつ安全なトラブルシューティングの手段
－　参照カテゴリに関する適用上の情報
－　関連する場合，試験間隔のチェック

SRP/CS のカテゴリ（又は複数の場合各カテゴリ）及びパフォーマンスレベルに関して，次のような特定の情報を提供しなければならない。

－　この規格の参照及び発行年号（すなわち，“**JIS B 9705-1**:2011”）
－　カテゴリ B，1，2，3 又は 4
－　パフォーマンスレベル，a，b，c，d 又は e

例　この規格に準拠して SRP/CS が，カテゴリ B で，かつ，パフォーマンスレベルが a の場合，次のように示す。

JIS B 9705-1:2011　カテゴリ B PL a

附属書 A
（参考）
要求パフォーマンスレベル PL_r の決定

A.1　PL_r の選択

この附属書は，考慮される制御システムの安全関連部によるリスク低減への寄与に関係する。ここで示す方法は，リスク低減の見積りだけを提供し，また，SRP/CS で必要な各安全機能に対して設計者及び規格作成者が PL_r を決定するための指針としての役割を意図している。

リスクアセスメントは，意図する安全機能の設定前の状況を想定する。意図する安全機能の PL_r を決定する際に，制御システムから独立した他の技術方策によるリスク低減（例えば，機械式ガード），又は追加安全機能によるリスク低減を考慮することができる。いずれの場合も，これら方策を実施した後（**図 2** 参照）に，**図 A.1** の開始点を選択することが可能である。

傷害のひどさ（S で示す）は，比較的容易に見積ることができる（例えば，裂傷，切断，致命傷）。発生頻度に関しては，補助パラメータがその見積り改善に使用される。これらのパラメータは，次による。

－　危険源への暴露頻度及び時間（F）

－　危険源回避又は危害の制限の可能性（P）

これらのパラメータは**図 A.1** に示すように“低”～“高”までリスクの段階的変化として組み合せることが経験上から可能である。これは，リスク見積りだけの定性的プロセスであることを強調している。

A.2　リスク見積りにおけるパラメータ S，F 及び P 選択の指針

A.2.1　傷害のひどさ S1 及び S2

安全機能の故障によって生じるリスク見積りでは，軽傷（通常，回復可能）及び重傷（通常，回復不可能）及び死亡だけを考慮する。

決定のために，通常，事故の重大性及び正常状態への回復過程を S1 及び S2 の決定では考慮することが望ましい。例えば，単純な打撲傷及び／又は裂傷は S1 に分類され，一方，切断又は死亡は S2 に分類されることになる。

A.2.2　危険源への暴露頻度及び／又は暴露時間 F1 及び F2

一般的に，パラメータ F1 又はパラメータ F2 を選択するための妥当な時間を特定することはできない。しかし，疑問が生じる場合，次の説明をすることによって，決定を容易にすることがある。

人が頻繁に，又は継続的に危険源に暴露される場合，F2 を選択することが望ましい。同一，又は異なる人のいずれが，継続的に危険源に暴露されているかは無関係である（例えばリフトの使用）。頻度のパラメータは，危険源への頻度及び接近時間に従って選択することが望ましい。

安全機能の動作要求頻度が設計者によって既知である場合，その要求頻度及び要求時間を危険源への接近頻度及び接近時間の代わりに，選択することができる。この規格では，安全機能の動作要求頻度は，1 年に 1 回以上を想定している。

危険源への暴露の期間は，設備使用時間の合計と関連させて，平均値をベースとして評価することが望ましい。例えば，ワークピースを搬入及び移動するようなサイクル運転中に機械のツール間に定期的に入ることが必要な場合，F2 を選択することが望ましい。もし機械への接近が時々必要であるという程度なら，F1 を選択できる。

注記　頻度が 1 時間に 1 回を超える場合で他に正当化を行えない場合は，F2 を選択することが望ましい。

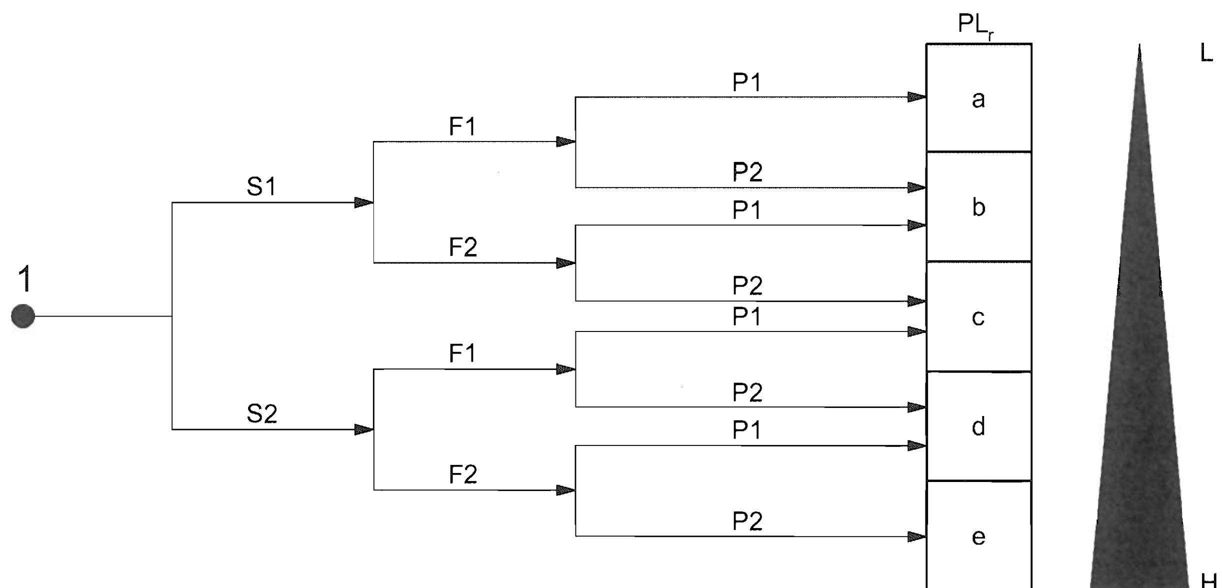
A.2.3　危険源回避の可能性 P1 及び P2

事故が起こる前に，危険状態を認知し，回避することができるかどうかを知ることは重要である。例えば，危険源を直接その物理的特性によって同定できるのか，又は，例えば表示装置のような技術的手段によってだけ認知できるのか，それを検討しておくことは重要である。パラメータ P の選択に影響する他の重要な要素は，例えば，次を含む。

- 監督付き又はなしの運転
- 熟練者又は非専門者による運転
- 危険源発生の速度（例えば，直ちに又はゆっくり）
- 危険源回避の可能性（例えば，脱出）
- 工程に関する実際の安全経験

危険状態が発生して，事故を回避する又はその効果を顕著に低減するための現実的機会が存在する場合だけ P1 を選択することが望ましい。危険源回避の可能性がほとんどない場合は P2 を選択することが望ましい。

図 A.1 に，リスクアセスメントによる安全関連 PL_r を決定するための指針を示す。グラフは，各安全機能に対して考慮することが望ましい。リスクアセスメントの方法は，**JIS B 9702** に基づき，かつ，**JIS B 9700-1** に従うことが望ましい。



記号の説明

1　リスク低減に安全機能の寄与度を評価するための開始点
L　リスク低減への寄与度“低”
H　リスク低減への寄与度“高”
PL_r　要求パフォーマンスレベル
S　傷害のひどさ
S1　軽症（通常，回復可能な傷害）
S2　重傷（通常，回復不可能又は死亡）
F　危険源への暴露の頻度及び／又は時間
F1　まれ～低頻度，及び／又はさらされる時間が短い
F2　高頻度～連続，及び／又はさらされる時間が長い
P　危険源回避又は危害の制限の可能性
P1　特定の条件下で可能
P2　ほとんど不可能

図 A.1－安全機能に対する要求 PL_r 決定のためのリスクグラフ

附属書 B
（参考）
ブロックメソッド及び安全関連ブロックダイアグラム

B.1 ブロックメソッド

この単純化した方法は，SRP/CS についてブロック指向の論理的表現を必要とする。SRP/CS は，次に従って，少数のブロックに分類することが望ましい。

－ ブロックは，安全機能の実行に関連する SRP/CS の論理ユニットを表す。
－ 安全機能を遂行する異なるチャネルは，異なるブロックに分離することが望ましい。もし一つのブロックがその機能を遂行できない場合，他のチャネルのブロックによる安全機能の実行に影響しないこと。
－ 各チャネルは，一つ又は複数のブロックで構成される場合がある。指定アーキテクチャ，入力，論理，及び出力における各チャネルごとの三つのブロックは，ブロック数を必須とするのではなく，各チャネル内の論理的な分離の例を単純に示す。
－ SRP/CS の各ハードウェアのユニットは，正確に一つのブロックに帰属させることが望ましい。それによって，そのブロックに帰属するハードウェアユニットの $MTTF_d$ に基づいたブロックの $MTTF_d$ を計算できる（例えば，FMEA 又はパーツ・カウント・メソッドによる。**D.1** 参照）。
－ 診断に使用されるだけのハードウェアユニット（例えば，試験装置）で，かつ，別のチャネルの安全機能の実行に影響を与えないハードウェアユニットは，それらが危険側に故障する場合，別のチャネルの安全機能の実行に必要なハードウェアユニットから分離してよい。

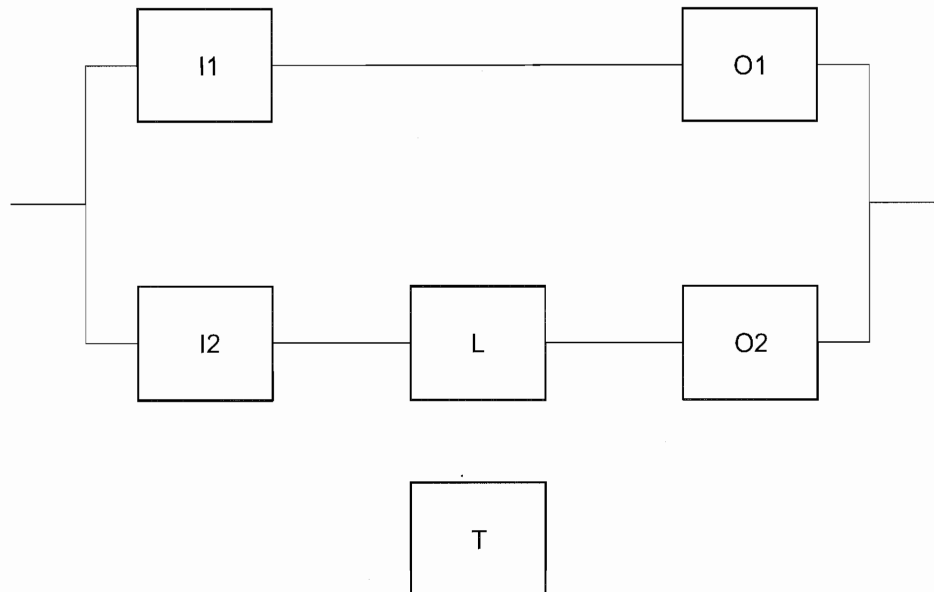
注記 この規格では，“ブロック”は，ファンクションブロック又は信頼性ブロックに対応してはいない。

B.2 安全関連ブロックダイアグラム

ブロックメソッドによって定義されたブロックは，安全関連ブロックダイアグラムでの SRP/CS の論理構造を作図によって表すために使用してよい。このような作図による表現に対しては，次の指針を適用できる。

－ 直列に配置された一つのブロックの故障がチャネル全体の故障につながる（例えば，SRP/CS の 1 チャネルのうち一つのハードウェアユニットが危険側故障を生じる場合，チャネル全体は，もはや安全機能を実行することができない場合がある。）
－ 並列に配置されたブロックの全てのチャネルの危険側故障だけが安全機能の喪失につながる（例えば，複数のチャネルによって遂行される安全機能は，少なくとも 1 チャネルが故障をしていない場合，その機能を実行できる。）。
－ 試験目的だけに使用されるブロックで，かつ，別のチャネルの安全機能の実行に影響を与えないブロックは，それが危険側に故障する場合，別のチャネルのブロックから分離してよい。

例は，**図 B.1** 参照



I1 及び O1 は，第 1 チャネルを構成する（直列配置）。I2，L 及び O2 は，第 2 チャネルを構成する（直列配置）。両チャネルをもつことによって，冗長化して安全機能を実行する（並列配置）。T は，試験のためだけに使用される。

記号の説明

I1，I2　入力装置，例えば，センサ

L　論理処理

O1，O2　出力装置，例えば，主接触器

T　試験装置

図 B.1－安全関連ブロックダイアグラムの例

附属書 C
（参考）
単一コンポーネントの $MTTF_d$ 値の計算又は評価

C.1　一般要求事項

この附属書は，単一コンポーネントの $MTTF_d$ 値を計算又は評価するために複数の方法を示す。すなわち，**C.2** に示す方法は，異なる種類のコンポーネントに対するグッド・エンジニアリング・プラクティスの考慮に基づいている。**C.3** に示す方法は，液圧式コンポーネントに適用可能である。**C.4** は，B_{10}（**C.4.1** 参照）による空圧式，機械式及び電気機械式コンポーネントの $MTTF_d$ 値を計算する手段を提供する。**C.5** は，電気式コンポーネントの $MTTF_d$ 値のリストである。

C.2　グッド・エンジニアリング・プラクティスメソッド

次の基準を満たす場合，コンポーネントの $MTTF_d$ 又は B_{10d} の値は，**表 C.1** に従って見積ることができる。

a) コンポーネントは，**ISO 13849-2** に示す基本安全原則及び“十分吟味された”安全原則，又はコンポーネントの設計のための関連規格（**表 C.1** 参照）に従って，製造されている（コンポーネントのデータシートにおける確認）。

　注記　この情報は，コンポーネント製造業者のデータシートで見ることができる。

b) コンポーネントの製造業者は，使用者に対して適切な用途及び運転条件を指定している。

c) SRP/CS の設計は，コンポーネントの実装及び運転に対して，**ISO 13849-2** で示される基本安全原則及び“十分吟味された”安全原則を満たしている。

C.3　液圧式コンポーネント

次の基準を満たす場合，単一液圧式コンポーネント，例えば，バルブの $MTTF_d$ 値は，150 年と見積ることができる。

a) 液圧式コンポーネントは，**ISO 13849-2** における液圧式コンポーネント設計のための**表 C.1** 及び**表 C.2** に示す基本安全原則及び“十分吟味された”安全原則に従って，製造されている（コンポーネントのデータシートにおける確認）。

　注記　この情報は，コンポーネント製造業者のデータシートで見ることができる。

b) 液圧式コンポーネントの製造業者は，使用者に対して適切な用途及び運転条件を指定している。SRP/CS の製造業者は，液圧式コンポーネントの実装及び運転に対して **ISO 13849-2** の**表 C.1** 及び**表 C.2** に従った基本安全原則及び“十分吟味された”安全原則を適用し，責任相応の情報を提供しなければならない。

a)又は **b)**のいずれかを達成できない場合，単一液圧式コンポーネントの $MTTF_d$ 値を，製造業者は提供しなければならない。

表 C.1－コンポーネントの $MTTF_d$ 又は B_{10d} を扱う国際規格，JIS 及びその他の規格

	ISO 13849-2 における基本安全原則及び“十分吟味された”安全原則	他の関連規格	代表値 $MTTF_d$（年） B_{10d}（サイクル）
機械式コンポーネント	表 A.1 及び表 A.2	－	$MTTF_d$＝150
液圧式コンポーネント	表 C.1 及び表 C.2	JIS B 8361 EN 982	$MTTF_d$＝150
空圧式コンポーネント	表 B.1 及び表 B.2	JIS B 8370 EN 983	B_{10d}＝20 000 000
リレー及び接触器 低負荷 （機械的負荷）	表 D.1 及び表 D.2	EN 50205 IEC 61810 規格群 JIS C 8201 規格群	B_{10d}＝20 000 000
リレー及び接触器 最大負荷	表 D.1 及び表 D.2	EN 50205 IEC 61810 規格群 JIS C 8201 規格群	B_{10d}＝400 000
近接スイッチ 低負荷 （機械的負荷）	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10d}＝20 000 000
近接スイッチ 最大負荷	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10d}＝400 000
接触器 低負荷 （機械的負荷）	表 D.1 及び表 D.2	JIS C 8201 規格群	B_{10d}＝20 000 000
接触器 定格負荷	表 D.1 及び表 D.2	JIS C 8201 規格群	B_{10d}＝20 000 00
位置スイッチ 負荷の考慮なし [a)]	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10d}＝20 000 000
位置スイッチ（別のアクチュエータ，施錠装置付き） 負荷の考慮なし [a)]	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10d}＝20 000 00
非常停止装置 負荷の考慮なし [a)]	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9703	B_{10d}＝100 000
非常停止装置（最大運転要求）[a)]	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9703	B_{10d}＝6 050
押しボタン （例えば，イネーブルスイッチ。負荷の考慮なし）[a)]	表 D.1 及び表 D.2	JIS C 8201 規格群	B_{10d}＝100 000

B_{10} の定義及び使用に関しては，**C.4** 参照。

注記 1　B_{10d} は，B_{10} の 2 倍で見積る（50 %の危険側故障）。

注記 2　“低負荷”は，例えば，定格値の 20 %を意味する（更なる情報は，**ISO 13849-2** 参照）。

注 [a)]　直接開離動作の障害の除外が可能な場合。

C.4　液圧式，機械式及び電気機械式コンポーネントの $MTTF_d$

C.4.1　一般要求事項

液圧式，機械式及び電気機械式のコンポーネント（液圧バルブ，電磁リレー，接触器，位置スイッチ，位置スイッチのカムなど）に対しては，この規格で要求され，かつ，年単位での危険側故障の平均時間（コンポーネントの $MTTF_d$）を計算することが困難な場合がある。大抵の場合，この種のコンポーネントの製造業者は，コンポーネントの 10 %が危険側故障に至る（B_{10d}）までの平均のサイクル数だけを示している。

この箇条では，用途に応じたサイクルに密接に関連して，製造業者によって示される B_{10d} 又は T（ライフタイム）の使用によるコンポーネントの $MTTF_d$ の計算方法を示す。

次の基準を満たす場合，単一の液圧式，電気機械式，又は機械式コンポーネントの $MTTF_d$ 値は，**C.4.2** に従って見積りすることができる。

a) コンポーネントは，その設計に関して **ISO 13849-2** の**表 B.1** 又は**表 D.1** による基本安全原則に従って，製造されている（コンポーネントのデータシートにおける確認）。

注記 この情報は，コンポーネント製造業者のデータシートで見ることができる。

b) カテゴリ 1，2，3 又は 4 で使用されるコンポーネントは，その設計に関し，**ISO 13849-2** の**表 B.2** 又は**表 D.2** による“十分吟味された安全原則”に従って製造されている（コンポーネントのデータシートにおける確認）。

注記 この情報は，コンポーネント製造業者のデータシートで見ることができる。

c) コンポーネントの製造業者は，使用者に対して適切な用途及び運転条件を指定している。SRP/CS の製造業者は，コンポーネントの実装及び運転に対して **ISO 13849-2** の**表 B.1** 及び**表 D.1** に従った基本安全原則を満たし，責任相応の情報を提供しなければならない。カテゴリ 1，2，3 又は 4 に関して，使用者はコンポーネントの搭載及び運転に対して **ISO 13849-2** の**表 B.2** 又は**表 D.2** に従った“十分吟味された安全原則”を満たし，自身の責任相応の情報を提供しなければならない。

C.4.2 B_{10d} によるコンポーネントの $MTTF_d$ の計算

コンポーネントの 10 %が危険側故障を生じるまでの平均サイクル数（B_{10d}）[1] を，試験方法のための関連製品規格（例えば，**JIS C 8201-5-1**，**ISO 19973** 規格群，**IEC 61810** 規格群）に従ってコンポーネントの製造業者は決定することが望ましい。コンポーネントの危険側故障モードを定義しなければならない。例えば，終端位置での固着又は開閉回数の変化など。試験において，全てのコンポーネントが危険側故障を生じるとは限らない場合（例えば，七つのコンポーネントの試験で，五つのコンポーネントだけが危険側に故障した），危険側故障を生じないコンポーネントを考慮して解析を実施することが望ましい。

B_{10d} [1] 及び n_{op}（年間の平均運転回数）によって，次のようにコンポーネントの $MTTF_d$ を計算することができる。

注 [1] B_{10} の危険側故障の割合が示されていない場合，$B_{10d}=2B_{10}$ の推奨として B_{10} の 50 %を使用する場合がある

$$MTTF_d = \frac{B_{10d}}{0.1 \times n_{op}} \qquad \text{(C.1)}$$

ここに，

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600 \text{ s/h}}{t_{cycle}} \qquad \text{(C.2)}$$

とし，コンポーネントの適用に対して次を設定する。

h_{op}： 平均運転回数（1 日当たりの時間数）

d_{op}： 平均運転回数（1 年当たりの日数）

t_{cycle}： コンポーネントの連続 2 サイクルでの開始と開始の間の平均時間（サイクル当たりの秒数）

コンポーネントの運転回数は，T_{10d} に制限される。コンポーネントの 10 %が危険側故障に至るまでの平均時間は，次のとおりである。

$$T_{10d} = \frac{B_{10d}}{n_{op}} \qquad \text{(C.3)}$$

注記 **C.4.2** に式の説明がある。

コンポーネントの 10 %が危険側に故障するまでのサイクルの平均回数 B_{10d} は，年間の平均運転回数 n_{op} を使用して，次のように，コンポーネントの 10 %が危険側に故障するまでの平均時間 T_{10d} に変換できる。

$$T_{10d} = \frac{B_{10d}}{n_{op}} \quad \text{(C.4)}$$

この規格の信頼性の方法は，コンポーネントの故障が長期的には指数関数［$F(t)=1-\exp(-\lambda_{dt})$］として分布することを仮定している。液圧式及び電気機械式コンポーネントに対しては，ワイブル分布がより好ましい。しかし，コンポーネントの運転時間は，コンポーネントの 10 %が危険側故障を生じるまでの平均時間（T_{10d}）に限定される。その際，この運転時間中での危険側の一定故障率（λ_d）は次のように見積ることができる。

$$\lambda_d = \frac{0.1}{T_{10d}} = \frac{0.1 \times n_{op}}{B_{10d}} \quad \text{(C.5)}$$

等式(C.5)は，一定の故障率で，コンポーネントの 10 %が，B_{10d}（サイクル）に対応して T_{10d}（年）後に故障するということを考慮している。正確には，次のとおりである。

$$F(T_{10d}) = 1 - \exp(-\lambda_d T_{10d}) = 10\ \%,\ \text{すなわち，}\ \lambda_d = \frac{\ln(0.9)}{T_{10d}} = \frac{0.105\,36}{T_{10d}} \fallingdotseq \frac{0.1}{T_{10d}} \quad \text{(C.6)}$$

指数分布に対して，$\mathrm{MTTF_d} = 1/\lambda_d$ とすると，次のとおりとなる。

$$\mathrm{MTTF_d} = \frac{T_{10d}}{0.1} = \frac{B_{10d}}{0.1 \times n_{op}} \quad \text{(C.7)}$$

C.4.3 例

液圧バルブに対しては，製造業者は B_{10d} として 60 万サイクルの平均値を確定する。バルブは，年間 220 日の運転回数でそれぞれ 1 日に 2 シフトで使用される。バルブの連続 2 サイクルでの開始と開始の間の平均時間（サイクル当たりの秒数）は，5 秒として見積る。これによって次の値を算出できる。

- d_{op}： 年 220 日間
- h_{op}： 日 16 時間
- T_{cycle}： サイクル当たり 5 秒
- B_{10d}： 60 万サイクル

この入力データによって，次の数値を算定できる。

$$n_{op} = \frac{200\text{日／年} \times 16\text{時間／日} \times 3\,600\text{秒／時間}}{5\text{秒s／サイクル}} = 2.53 \times 10^6\ \text{サイクル／年} \quad \text{(C.8)}$$

$$T_{10d} = \frac{60 \times 10^6\ \text{サイクル}}{2.53 \times 10^6\ \text{サイクル／年}} = 23.7\ \text{年} \quad \text{(C.9)}$$

$$\mathrm{MTTF_d} = \frac{23.7\ \text{年}}{0.1} = 237\ \text{年} \quad \text{(C.10)}$$

この数値は，**表 5** によって，コンポーネントの $\mathrm{MTTF_d}$ として“高”となる。この仮定は，バルブに対しては 23.7 年の制限付き運転時間だけが有効である。

C.5 電気式コンポーネントの $\mathrm{MTTF_d}$ データ

C.5.1 一般要求事項

表 C.2～**表 C.7** に，電気式コンポーネントに対する $\mathrm{MTTF_d}$ の代表的な平均値を示す。データは **SN 29500**

シリーズのデータベース（参考文献の[51]）から抜粋してある。全てのデータは，一般的な形式のものである。種々の電気式コンポーネントに対する $MTTF_d$ 値を示す種々のデータベースが利用可能である（参考文献のデータベースリスト参照)。SRP/CS の設計者で，使用のコンポーネントに関する他の信頼できる特定のデータを所有する場合，その特定のデータの使用を強く推奨する。

表 C.2～**表 C.7** に示す値は，定格の電流及び電圧で 40 ℃の温度に対して有効である。

表の MTTF の欄には，一般的コンポーネントで必ずしも危険側障害ではない潜在的故障モードの全てについて **SN 29500** から引用した値が示してある。表の $MTTF_d$ の欄は，故障モードの全てが必ずしも危険側故障に至るとはしないことを代表的に仮定している。これは主として用途による。コンポーネントの“代表的” $MTTF_d$ を決定するための適確な方法は，FMEA を実施することである。ある種のコンポーネント，例えば，スイッチとして使用するトランジスタは，故障として回路短絡又は断路を生じる場合がある。この二つのモードのうちで一方だけ危険側となる場合がある。したがって，“留意事項”の欄には 50 %の危険側障害だけを仮定して，コンポーネントの $MTTF_d$ は MTTF 値の 2 倍となることを意味する。疑わしい使用に対しては，安全マージンを 10 倍として最悪ケースの $MTTF_d$ を右欄に示してある。

C.5.2　半導体

表 C.2 及び**表 C.3** による。

表 C.2－トランジスタ（スイッチング用）

トランジスタ	例	MTTF［年］	$MTTF_d$［年］		留意事項
			代表値	最悪ケース	
バイポーラ	TO18，TO92，SOT23	34 247	68 493	6 849	危険側故障 50 %
バイポーラ，（低電力用）	TO5，TO39	5 708	11 416	1 142	危険側故障 50 %
バイポーラ，（電力用）	TO3，TO220，D-Pack	1 941	3 881	388	危険側故障 50 %
FET	接合 MOS	22 831	45 662	4 566	危険側故障 50 %
MOS（電力用）	TO3，TO220，D-Pack	1 142	2 283	228	危険側故障 50 %

表 C.3－ダイオード，パワー半導体及び半導体集積回路

ダイオード	例	MTTF［年］	$MTTF_d$［年］		留意事項
			標準値	最悪の場合	
一般目的	－	114 155	228 311	22 831	危険側故障 50 %
サプレッサ	－	15 981	31 963	3 196	危険側故障 50 %
ツェナーダイオード Ptot＜1 W	－	114 155	228 311	22 831	危険側故障 50 %
整流ダイオード	－	57 078	114 155	11 416	危険側故障 50 %
整流ブリッジ	－	11 415	22 831	2 283	危険側故障 50 %
サイリスタ	－	2 283	4 566	457	危険側故障 50 %
トライアック，ダイアック	－	1 484	2 968	297	危険側故障 50 %
半導体集積回路（プログラマブル及び非プログラマブル）	製造業者のデータを使用				危険側故障 50 %

C.6　受動素子

表 C.4～表 C.7 による。

表 C.4－コンデンサ

コンデンサ	例	MTTF［年］	MTTF$_d$［年］		留意事項
			標準値	最悪の場合	
標準，（電力使用でない場合）	KS，KP，KC，KT，MKT，MKC，MKP，MKU，MP，MKV	57 078	114 155	11 416	危険側故障 50 %
セラミック	－	22 831	45 662	4 566	危険側故障 50 %
アルミニウム（電解式）	非固体電解質	22 831	45 662	4 566	危険側故障 50 %
アルミニウム（電解式）	固体電解質	37 671	75 342	7 534	危険側故障 50 %
タンタル（電解式）	非固体電解質	11 415	22 831	2 283	危険側故障 50 %
タンタル（電解式）	固体電解質	114 155	228 311	22 831	危険側故障 50 %

表 C.5－抵抗器

抵抗器	例	MTTF［年］	MTTF$_d$［年］		留意事項
			標準値	最悪の場合	
炭素フィルム	－	114 155	228 311	22 831	危険側故障 50 %
金属フィルム	－	570 776	1 141 552	114 155	危険側故障 50 %
酸化金属及びワイヤ巻き	－	22 831	45 662	4 566	危険側故障 50 %
可変式	－	3 767	7 534	753	危険側故障 50 %

表 C.6－誘導子

誘導子	例	MTTF［年］	MTTF$_d$［年］		留意事項
			標準値	最悪の場合	
MC 用	－	37 671	75 342	7 534	危険側故障 50 %
低周波数誘導子及び変圧器	－	22 831	45 662	4 566	危険側故障 50 %
主変圧器，スイッチモード及びパワー供給用変圧器	－	11 415	22 831	2 283	危険側故障 50 %

表 C.7－フォトカプラ

フォトカプラ	例	MTTF［年］	MTTF$_d$［年］		備考
			代表値	最悪の場合	
バイポーラ出力	SFH 610	7 648	15 296	1 530	危険側故障 50 %
FET 出力	LH 1056	2 854	5 708	571	危険側故障 50 %

附属書D
（参考）
チャネルごとの$MTTF_d$を見積るための簡易的な方法

D.1 パーツ・カウント・メソッド

“パーツ・カウント・メソッド”の使用は，各チャネルごとの$MTTF_d$見積りに使用する。チャネルの一部をなす単一コンポーネントの全ての$MTTF_d$値をこの計算に使用する。

一般的な式は，次の式(D.1)のとおりである。

$$\frac{1}{MTTF_d}=\sum_{i=1}^{\tilde{N}}\frac{1}{MTTF_{di}}=\sum_{i=1}^{\tilde{N}}\frac{n_j}{MTTF_{dj}} \qquad \text{(D.1)}$$

ここに，　$MTTF_d$：　1チャネル全体の平均危険側故障率

$MTTF_{di}$，$MTTF_{dj}$：　安全機能に寄与する各コンポーネントの$MTTF_d$

最初の合計は，各コンポーネントを個別に分割しており，次の合計は，同一の$MTTF_{dj}$をもつn_j個のコンポーネントの全てが一緒にグループ化される場合で，単純化してある。

例

$1/MTTF_{di}=1/30+1/30+1/30$

$nj/MTTF_{dj}=3/30=1/10$

表D.1の例は，21.4年のチャネルの$MTTF_d$を示しており，この$MTTF_d$は，**表5**に従って“中”である。

表D.1－回路基板の部品リストの例

J	コンポーネント	ユニット nj	$MTTF_{dj}$ 最悪の場合 ［年］	$1/MTTF_{dj}$ 最悪の場合 ［1/年］	$nj/MTTF_{dj}$ 最悪の場合 ［1/年］
1	トランジスタ，バイポーラ，低電力使用（**表C.2**参照）	2	1 142	0.000 876	0.001 752
2	抵抗器，炭素フィルム（**表C.5**参照）	5	22 831	0.000 044	0.000 219
3	コンデンサ，標準形，電力使用でない（**表C.4**参照）	4	11 416	0.000 088	0.000 350
4	リレー（低負荷，**C.1**参照）（B_{10d}＝20 000 000サイクル，n_{op}＝633 600）	4	315.66	0.003 168	0.012 672
5	電磁接触器（定格負荷，**C.1**参照）（B_{10d}＝20 000 000サイクル，n_{op}＝633 600）	1	31.57	0.031 676	0.031 676
$\sum(nj/MTTF_{dj})$					0.046 669
$MTTF_d=1/\sum(nj/MTTF_{dj})$　［年］		21.43			

注記1　この方法は，あるチャネル内のコンポーネントの危険側故障がそのチャネル全体の危険側故障を導くという仮定に基づいている。**表D.1**で示される$MTTF_d$の計算は，これに基づく。

注記2　この例では，主な影響は，接触器から生じる。この例の$MTTF_d$及びB_{10}の値は，**附属書C**に基づく。例えば，d_{op}＝220日／年，h_{op}＝8時間／日，及びt_{cycle}＝10秒／サイクルを仮定し，n_{op}＝633 600サイクル／年を示す。一般的に，製造業者が提供する$MTTF_d$及びB_{10d}の値を採用することは，**附属書C**の**表C**で示される値を採用するよりもよい結果につながる。つまり，そのチャネルの$MTTF_d$をより高めることを意味する。

D.2　異なるチャネルに対する $MTTF_d$ と，各チャネルの $MTTF_d$ の対称化

6.2 の指定アーキテクチャは，冗長の SRP/CS における異なるチャネルについて，各チャネルの $MTTF_d$ の値が同じであることを仮定している。このチャネルごとの値を，**図 5** の入力データにすることが望ましい。

チャネル間の $MTTF_d$ が異なる場合には，次の二つの可能性がある。

－　最悪の場合の仮定として，低い方の値を考慮することが望ましい，又は

－　$MTTF_d$ の代用値の見積りとして，式(D.2)を使用する。

$$MTTF_d = \frac{2}{3}MTTF_{dC1} + MTTF_{dC2} = \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \quad \cdots\cdots (D.2)$$

ここで，$MTTF_{dC1}$ 及び $MTTF_{dC2}$ は，異なる冗長チャネルの $MTTF_d$ 値である。

式の例：

一方のチャネルが $MTTF_{dC1}$＝3 年を，他方のチャネルが $MTTF_{dC2}$＝100 年をもつ場合の結果は，$MTTF_d$＝66 年である。このことは，一方のチャネルに 100 年の $MTTF_d$ 及び他方のチャネルに 3 年の $MTTF_d$ をもつ冗長システムは，それぞれのチャネルが 66 年の $MTTF_d$ をもつシステムに等しいことを意味している。

2 チャネルをもち，かつ，各チャネルの $MTTF_d$ 値が異なる冗長システムは，式(D.2)を使用して，各チャネルで同一の $MTTF_d$ をもつ冗長システムとして置き換えることができる。この手順は，**図 5** を正確に使用するために必要とされる。

注記　この方法は，独立した並列チャネルを仮定している。

附属書 E
(参考)
機能及びモジュールの診断範囲（DC）の見積り

E.1　診断範囲（DC）の例

表 E.1 による。

表 E.1－診断範囲（DC）の見積り

方策		DC
EI	入力装置	
1	入力信号の動的（ダイナミックな）変化による周期的試験	90 %
2	もっともらしさ（プラウザビリティ）チェック，例えば，ノーマルオープン及びノーマルクローズの機械的結合接点使用	99 %
3	動的試験なしの入力装置の相互監視	適用ごとに，信号の切替頻度がどの程度頻繁に行われるかによって 0 %～99 %に変動する。
4	回路短絡を検出できない場合，動的試験付きの入力信号の相互監視（マルチ I/O に対して）	90 %
5	入力信号及び論理（処理）（L）内の中間結果の相互監視，プログラムフローの一時的及び論理的ソフトウェア監視，並びに静的障害及び回路短絡の検出（マルチ I/O に対して）	99 %
6	間接監視（例えば，圧力スイッチによる監視，アクチュエータの電気的位置監視）	適用によって，90 %～99 %に変動する。
7	直接監視（例えば，制御バルブの電気的位置監視，機械的結合接点要素による電気機械装置の監視）	99 %
8	処理による障害検出	適用によって，0 %～99 %に変動する。この方策だけでは，要求パフォーマンスレベル“e”に対しては十分でない。
9	センサのある種の特性監視（応答時間，アナログ信号の範囲，例えば電気抵抗，静電容量）	60 %
EL	論理	
1	間接監視（例えば，圧力スイッチによる監視，アクチュエータの電気的位置監視）	適用によって，90 %～99 %に変動する。
2	直接監視（例えば，制御バルブの電気的位置監視，機械的結合接点要素による電気機械装置の監視）	99 %
3	論理の単純な一時的時間経過の監視（例えば，ウォッチドッグとしてのタイマ。論理のプログラム内にトリガ点をもつ）	60 %
4	ウォッチドックによる一時的で，かつ，論理的監視。試験装置は論理の挙動に対するもっともらしさ（プラウザビリティ）チェック	90 %
5	論理（プログラム及びデータ記憶，入／出力ポート，インタフェース等）の部分に潜在する障害を検出するための起動時の自動試験（セルフテスト）	90 %（試験技術による）
6	主チャネルによる監視装置の応答能力のチェック（例えば，ウォッチドック）。起動時，又は安全機能の動作要求時，又は外部信号が入力装置を介してそれを要求するとき。	90 %
7	動的（ダイナミック処理）原則（安全機能の動作要求時に，論理の全てのコンポーネントにオン-オフ-オン状態の変化を要求する）。例えば，リレー実装のインタロック回路	99 %

表 E.1－診断範囲（DC）の見積り（続き）

方策		DC
8	不変メモリ：1 ワードによるシグネチャ（8 ビット）	90 %
9	不変メモリ：2 ワードによるシグネチャ（16 ビット）	99 %
10	可変メモリ：冗長データ，例えば，フラッグ，マーカ，定数，タイマ，及びこれらデータの相互比較，の使用による RAM テスト	60 %
11	可変メモリ：使用するデータメモリセルの読込み及び書出しのチェック	60 %
12	可変メモリ：変更ハミングコードの RAM 監視，又は RAM の自動監視（セルフテスト）（例えば，“galpat” 又は “abraham”）	99 %
13	処理ユニット：ソフトウェアによる自動試験（セルフテスト）	60 %～90 %
14	処理ユニット：コード化プロセス	90 %～99 %
15	処理による障害検出	適用によって，0 %～99 %に変動する。この方策だけでは，要求パフォーマンスレベル “e” を満足するのに十分ではない。
EO	出力装置	
1	動的試験なしの単一チャネルによる出力監視	適用ごとに，信号の切替頻度がどの程度頻繁に行われるかによって 0 %～99 %に変動する。
2	動的試験なしの出力の相互監視	適用ごとに，信号の切替頻度がどの程度頻繁に行われるかによって 0 %～99 %に変動する。
3	回路短絡検出なしの動的試験による出力の相互監視（マルチ I/O）	90 %
4	出力信号及び論理（L）内の中間結果の相互監視，プログラムフローの一時的，かつ，論理的ソフトウェアの監視，並びに静的障害及び回路短絡の検出（マルチ I/O）。	99 %
5	アクチュエータ監視なしの冗長化された遮断経路	0 %
6	論理又は試験装置によるアクチュエータのうちの一つを監視する冗長化遮断経路	90 %
7	論理及び試験装置によるアクチュエータを監視する冗長化遮断経路	99 %
8	間接監視（例えば，圧力スイッチによる監視，アクチュエータの電気的位置監視）	適用によって，90 %～99 %に変動する。
9	処理による障害検出	適用によって，0 %～99 %に変動する。この方策だけでは，要求パフォーマンスレベル “e” を満足するのに十分ではない。
10	直接監視（例えば，制御バルブの電気的位置監視，機械的に結合した接点要素による電気機械装置の監視）	99 %

注記 1 DC に対する追加の見積りは，例えば，**IEC 61508-2** の**表 A.2**～**表 A.15** 参照。

注記 2 DC “中” 又は DC “高” が論理に対して要求される場合，可変メモリ，不変メモリ，及び処理ユニットには，それぞれ少なくとも 60 %の DC をもつための，一方策（少なくとも）を適用しなければならない。DC の手法は，この表に掲げた方策とは別の方策の場合がある。

E.2　平均 DC（DCavg）の見積り

多くのシステムでは障害検出に対して複数の方策を使用することが可能である。これらの方策は SRP/CS の異なる部分をチェックして，かつ，異なる DC をもつことがある。**図 5** による PL の見積りでは，安全

機能を実行するSRP/CS全体に対して，ただ一つの“平均”のDCを適用することができる。

DC は，検出される危険側故障率と全危険側故障率間の比として定義することができる。この定義に従って，平均診断範囲DC_{avg}は，次の式(E.1)で見積る。

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}} \qquad \text{(E.1)}$$

ここに，障害の除外なしのSRP/CSの全コンポーネントを考慮して，かつ，加算しなければならない。各ブロックに対して，$MTTF_d$及びDCを考慮する。式(E.1)のDCは，（故障を検出するために使用される方策には無関係に）全危険側故障率に対して，この部分で検出される危険側故障率との比を意味している。このように，DC は試験される部分を指しており，試験装置を指してはいない。故障検出なしのコンポーネント（例えば，試験されない部分）は，DC＝0であって，DC_{avg}の分母の数値を提供するだけである。

附属書 F
（参考）
共通原因故障（CCF）の見積り

F.1　CCF に対する要求事項

センサ／アクチュエータ，及び，これらとは別の制御論理対応の CCF 方策に対する包括的な手順は，例えば，**IEC 61508-6** の**附属書 D** で示される。そこで示される方策の全てが，必ずしも機械類に適用可能ではない。ここでは最も重要な方策を列挙する。

注記　この規格では，**IEC 61508-6** の**附属書 D** に従って，冗長システムでの β ファクタは 2 %以下であることが望ましい。

F.2　CCF の影響の見積り

この定量的プロセスは，システム全体を通して実施することが望ましい。制御システムの全ての安全関連部を考慮するのがよい。**表 F.1** に，工学的判断に基づいて，共通原因故障を低減させるような方策を列挙し，かつ，関連の値を含める。

各方策に対しては，満点の得点又は零点だけを主張できる。方策が部分的にだけ満足する場合，その方策による得点は，零点である。

表 F.1－採点方法及び CCF に対する方策の定量化

No	CCF に対する方策	得点
1	分離／隔離	
	信号経路間の物理的な分離 　配線／配管での分離 　プリント基板上での回路間の十分なクリアランス及び沿面距離	15
2	多様性（ダイバーシティ）	
	異なる技術的方式／設計又は物理的原理の使用。例えば，第 1 チャネルはプログラマブル電子方式及び第 2 チャネルはハードワイヤ方式 始動の種類 圧力及び温度 距離及び圧力の測定 デジタル及びアナログ 異なる製造業者によるコンポーネント	20
3	設計／適用／経験	
3.1	過電圧，過圧力，過電流などに対する保護	15
3.2	使用のコンポーネントは，“十分吟味されている”	5
4	査定／分析	
	設計上での共通原因故障を回避するために，故障モード影響分析（FMEA）の結果を考慮しているか？	5
5	適格性（能力）／訓練	
	設計者／保全者は，共通原因故障の原因及び結果を理解できるように訓練されているか？	5

表 F.1－採点方法及び CCF に対する方策の定量化（続き）

No	CCF に対する方策	得点
6	環境面	
6.1	適切な規格に従った CCF に対する汚染防止及び電磁両立性（EMC） 流体システム：圧力媒体のろ過，ほこりの侵入の防止，圧縮空気の水抜き，例えば，圧力媒体の純度に関してはコンポーネント製造業者の要求事項に従う。 電気システム：システムは，電磁イミュニティに関してチェックされているか？例えば CCF に対する関連規格で規定されるように。 流体システムと電気システムとの組合せに対しては，これらの両面を考慮することが望ましい。	25
6.2	他の影響 温度，衝撃，振動，湿度（例えば，関連規格で規定されるように）などの環境関連の影響の全てに対してイミュニティの要求事項を考慮しているか？	10
	合計	（最大達成可能 100）

合計得点	CCF を回避するための方策 a)
65 以上	要求事項に適合
65 未満	要求事項に不適合 ⇒ 追加方策の選択

注 a) 技術方式上の方策が関連しない場合でも，この欄で算定された得点は，包括的な計算の際に考慮することができる。

附属書G
（参考）
システマティック故障

G.1　一般要求事項

基本安全原則及び“十分に吟味された”安全原則等のシステマティック故障に対して適用される包括的な方策リストは，**ISO 13849-2** で規定する。

G.2　システマティック故障の抑制に関する要求事項

次の方策を適用することが望ましい。

- エネルギ非供給状態の使用（**ISO 13849-2** 参照）
  制御システムの安全関連部（SRP/CS）は，動力供給の喪失で機械を安全状態にするか又は安全状態を維持できるように設計することが望ましい。
- 降伏電圧，電圧変動，過電圧，不足電圧の影響を抑制する方策
  降伏電圧，電圧変動，過電圧，不足電圧条件へ応答する SRP/CS の挙動をあらかじめ決めることが望ましい。それによって，SRP/CS は機械を安全状態にするか又は安全状態を維持できる（**JIS B 9960-1** 及び **IEC 61508-7** の **A.8** 参照）。
- 物理的環境の影響（例えば，温度，湿度，水，振動，ほこり，腐食性物質，電磁干渉及びその影響）を抑制又は回避する方策
  物理的環境の影響へ対応する SRP/CS の挙動をあらかじめ決定することが望ましい。それによって，SRP/CS が機械を安全状態にするか又は安全状態を維持できる（例えば，**JIS C 0920**，**JIS B 9960-1** 参照）。
- ソフトウェアを含む SRP/CS には，プログラムシーケンスの欠陥を検出するためにプログラムシーケンス監視を使用することが望ましい。
  プログラムの個々の要素（例えば，ソフトウェアモジュール，サブプログラム又はコマンド）が誤りのシーケンス若しくは周期時間で処理される場合，又はプロセッサのクロック信号に誤りがある場合に，欠陥をもつプログラムシーケンスが生じる（**IEC 61508-7** の **A.9** 参照）。
- データ通信プロセスから生じるエラーの影響及びその他の影響を抑制する方策（**IEC 61508-2** の **7.4.8** 参照）

さらに，SRP/CS の複雑さ及びその PL を考慮して，次の方策の一つ以上を適用しなければならない。

- 自動試験による故障検出
- 冗長ハードウェアによる試験
- 多様性（ダイバーシティ）・ハードウェア
- ポジティブモードによる操作
- 機械的に結合された接点
- 直接開離作用
- 非対称故障モード
- 適した係数による過大見積り（オーバディメンショニング）。製造業者は，ディレーティングを信頼性改善に適用してそれを証明することができ，その場合適切な諸元の過大見積りは，少なくとも 1.5 倍

の係数を使用することが望ましい。

ISO 13849-2 の **D.3** も参照。

G.3　システマティック故障を回避する方策

次の方策を適用することが望ましい。

- 適した材料及び適切な製造方法の使用

  例えば，応力，耐性，弾性，摩擦，摩耗，腐食，温度，導電性，絶縁耐力を考慮した材料，製造方法及び処理方法の選択

- 適切な寸法及び形状

  例えば，応力，張力，疲労，温度，表面の粗さ，許容公差，製造方法の考慮

- ケーブル接続，配線及び相互（内部）接続を含む，コンポーネントの正しい選択，組合，配置，組立及び据付

  適切な規格及び製造業者の適用上の留意事項，例えば，カタログ，据付指示書，仕様書，及びグッド・エンジニアリング・プラクティスの使用

- 互換性

  互換性のある操作特性をもつコンポーネントの使用

- 特定の環境条件への耐性

  全ての予想される環境条件及び予見可能な悪条件，例えば，温度，湿度，振動及び電磁障害（EMI），で作動することができるよう SRP/CS を設計する（**ISO 13849-2** の **D.2** 参照）。

- 適切な規格で設計され，かつ，明確に定義される故障モードをもつコンポーネントの使用

  特定の特性をもつコンポーネントの使用によって，未検出障害のリスクを低減させる（**IEC 61508-7** の **B.3.3** 参照）。

追加して，SRP/CS の複雑性及びその PL を考慮して，次の方策の一つ以上を適用する。

- ハードウェアのデザインレビュー（例えば，検査又はウォークスルーによる）

  レビュー及び分析によって仕様書と実装との間の矛盾を明らかにする（**IEC 61508-7** の **B.3.7** 及び **B.3.8** 参照）。

- シミュレーション又は分析が可能なコンピュータ支援設計ツール

  設計手順を系統的に実行し，かつ，既に利用され，試験されている適切な自動的構築要素を含む（**IEC 61508-7** の **B.3.5** 参照）。

- シミュレーション

  機能上の性能及びそのコンポーネントの正しい規模の両方に関して，SRP/CS 設計の系統的で完全な検査を実行する（**IEC 61508-7** の **B.3.6** 参照）。

G.4　SRP/CS を組み込む際のシステマティック故障の回避の方策

SRP/CS を組み込む際には，次の方策を適用することが望ましい。

- 機能試験
- プロジェクト管理
- 文書化

  さらに，SRP/CS の複雑さ及びその PL を考慮して，ブラックボックス試験を適用することが望ましい。

附属書 H
（参考）
制御システムにおける複数の安全関連部の組合せ例

図 H.1 は，機械アクチュエータを制御する機能の一つを示すための安全関連部の概念図である。同図は，機能又は動作を示すのでなく，この一機能のカテゴリ及び技術方式の組合せの原理だけを説明している。

制御系は，電子式制御論理及び液圧式方向制御バルブによって構成される。リスクは，AOPD によって低減されており，光ビームが遮断されると，危険状態へのアクセスが検知され，液圧アクチュエータの起動が防止される。

安全機能を提供する安全関連部は，AOPD，電子制御論理，液圧方向制御バルブ及び相互接続手段である。

この組合せによる安全関連部は，安全機能として停止機能を備えている。AOPD が遮断された場合，その出力は電子制御論理に発信され，電子制御論理は信号を液圧方向制御バルブへ伝送し，液圧方向制御バルブはその信号を SRP/CS の出力として受け取り，流体の流れを停止する。機械においては，これは液圧アクチュエータの危険な動きを停止することになる。

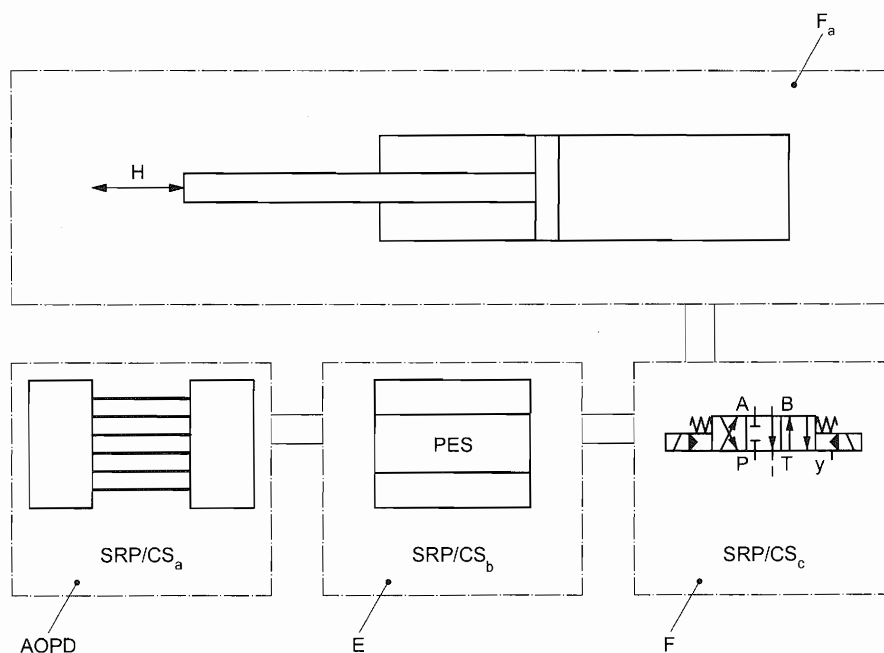
安全関連部のこの組合せは，箇条 **6** の要求事項に基づく異なるカテゴリ及び技術方式の組合せによって達成される安全機能の証明となる。この規格の原則を使用することによって，**図 H.2** で示される安全関連部は次のように述べることができる。

－ 電気検知保護装置（ライトカーテン）は，カテゴリ 2，PL＝c である。障害の発生確率を低減するために“十分吟味された”安全原則を使用する。
－ 電子式制御論理は，カテゴリ 3，PL＝d である。この電子式制御論理の安全性能レベルを向上させるために SRP/CS の構成を冗長系として，それによって単一障害のほとんどを検出することができるような複数の障害に対する検出方策を実施している。
－ 液圧方向制御バルブは，カテゴリ 1，PL＝c である。“十分吟味された”状態は，主に適用によって特定される。この例では，バルブが“十分吟味された”ものとして考えられている。障害の発生確率を低減するために，この装置は“十分吟味された”安全原則の使用の適用による“十分に吟味された”コンポーネントで構成され，かつ，全ての適用条件を考慮している（**6.2.4** 参照）。

注記 1　接続手段の位置，大きさ及びレイアウトも考慮しなければならない。

この組合せでは，PL_{low} が c であり（PL_{low}＝c），PL_{low} の数が 2（N_{low}＝2）なので，全パフォーマンスレベル PL は，c（PL＝c）となる（**6.3** 参照）。

注記 2　**図 H.2** でカテゴリ 1 又はカテゴリ 2 の部分に単一障害が発生した場合，安全機能を喪失する場合がある。



記号の説明

AOPD　能動的光電保護装置（例えば，ライトカーテン）。SRP/CS$_a$：カテゴリ 2［タイプ 2（**JIS B 9704-1**）］，PL＝c

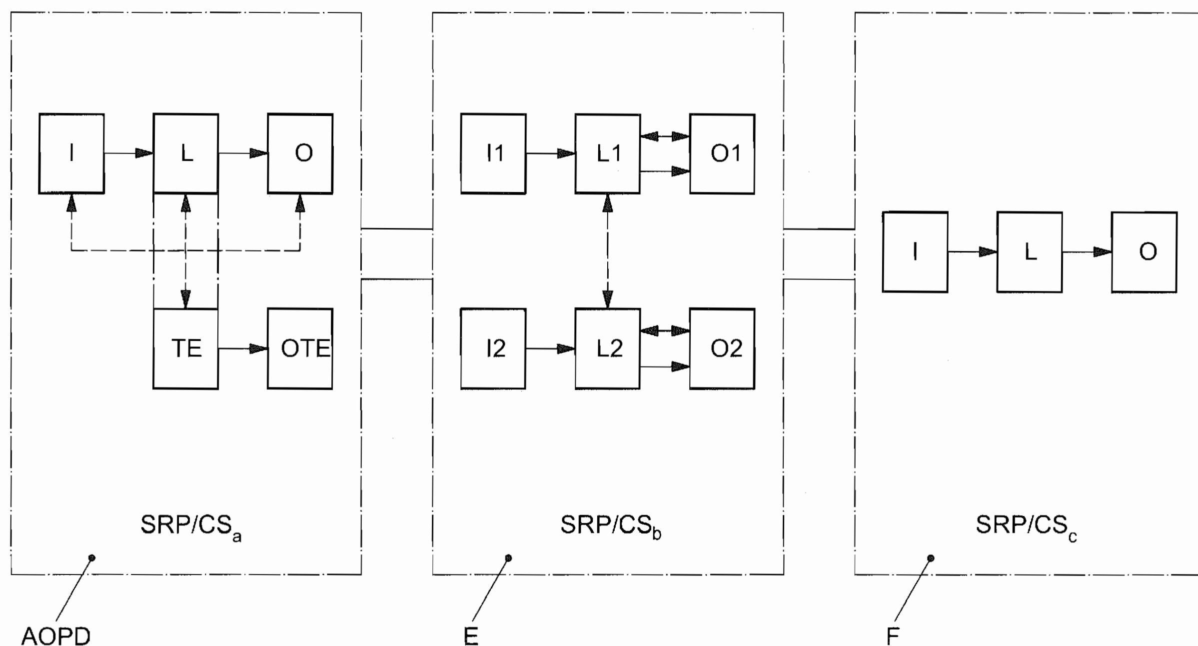
E　電子式制御論理による SRP/CS$_b$：カテゴリ 3，PL＝d

F　液圧式による SRP/CS$_c$：カテゴリ 1，PL＝c

F$_a$　液圧アクチュエータ

H　危険な動き

図 H.1－例－SRP/CS の組合せを説明するためのブロックダイアグラム



記号の説明
AOPD　　能動的光電保護装置（例えば，ライトカーテン）。
E　電子式制御論理系
F　液圧系
I，I1，I2　入力装置（例えば，センサ）
L，L1，L2　　　論理
O，O1，O2，OTE　　出力装置（例えば，主接触器）
TE　試験装置

図 H.2－指定アーキテクチャによる図 H.1 の具体的構成図

附属書 I
（参考）
事例

I.1　一般要求事項

この附属書では，安全機能を同定し，かつ，PL を決定するために，既に附属書で述べた方法の使用を例示する。一般的に使用される二つの制御回路の定量化を示す。ステップの手順は，**図 3** を参照。

二つの異なる制御回路の例 A 及び例 B を審査する。**図 I.1** 及び**図 I.3** を参照。両図共にインタロック付きガードのドアを有し，同じ安全機能の性能で示してある。最初の事例は，$MTTF_d$＝“高”の電気機械式コンポーネントの単一チャネルとして構成される。第 2 番目の事例は，2 チャネルシステムで構成されており，一方のチャネルは電気機械式，他方のチャネルは機能試験付のプログラマブル電子式で，$MTTF_d$が低いコンポーネントである。

I.2　安全機能及び要求パフォーマンスレベル PL_r

両事例に対して，インタロック付ガード装置の安全機能は，次のように選択することが可能である。

ガードの扉が開くと危険な動きは停止する（電気モータの無通電による）。

リスクグラフ法（**図 A.1** 参照）によるリスクパラメータは，次のとおりである。

－　傷害のひどさ：S＝S2（重症）
－　危険源への暴露頻度及び／又は暴露時間：F＝F1（まれ～低頻度，及び／又は暴露される時間は短い）
－　危険源回避の可能性：P＝P1（特定の条件で可能）

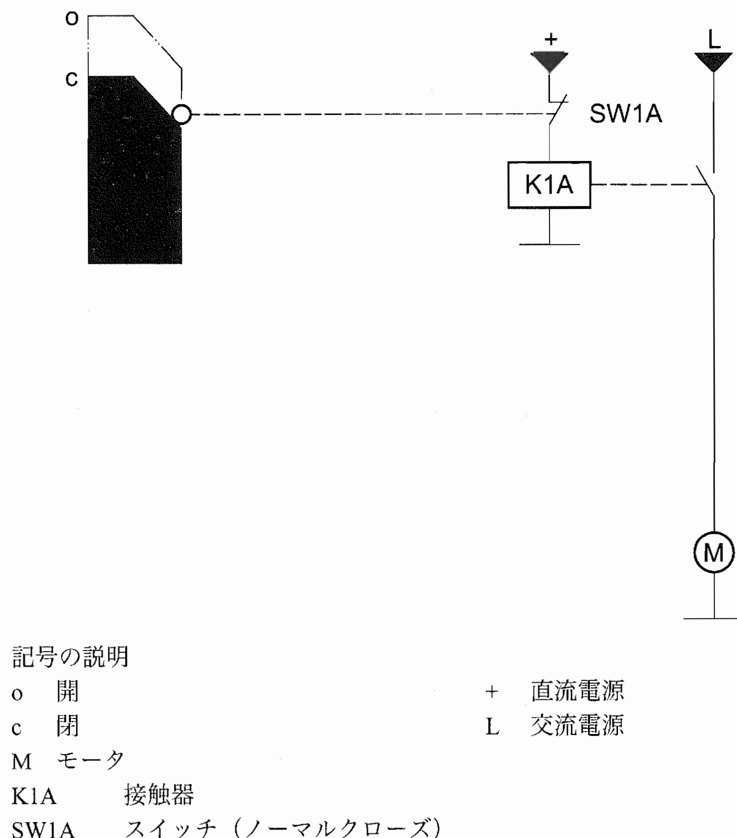
これらの三つの決定によって，要求パフォーマンスレベルは PL_r＝c となる。

推奨カテゴリの決定：パフォーマンスレベル c は，高く信頼できる単一チャネルシステム（カテゴリ 1），又は冗長系のアーキテクチャ（カテゴリ 2 又はカテゴリ 3）によって，達成することができる（**図 5** 及び**箇条 6** 参照）。

I.3　例 A，単一チャネルシステム

I.3.1　安全関連部の特定

安全機能に寄与する全てのコンポーネントは，**図 I.1** に示されている。インタロックの安全機能（起動及び停止スイッチとして）に寄与しない機能の詳細は，省略してある。



記号の説明

o	開	+	直流電源
c	閉	L	交流電源
M	モータ		
K1A	接触器		
SW1A	スイッチ（ノーマルクローズ）		

図 I.1－安全機能を遂行する制御回路 A

この例では，ドアスイッチはノーマルクローズの接点（しかし，正当化できる障害の除外はない。）をもち，かつ，モータへの電源を遮断できる接触器に次の構成で接続されている。

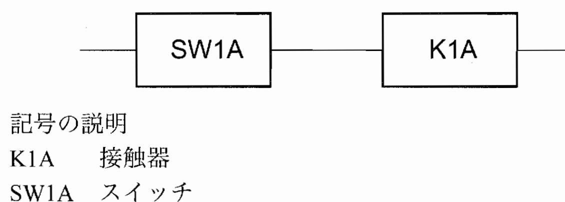
－　電気機械式コンポーネントの単一チャネル

－　スイッチ SW1A は，$MTTF_d$＝“中”である。

－　接触器 K1A は，$MTTF_d$＝“低”である。

この例で選択した接触器は，**ISO 13849-2** に従って実装する場合，“十分吟味された”コンポーネントである。

このように，安全関連部及びその各チャネルへの分割は，**図 I.2** で示すように，安全関連ブロックダイアグラムで図示できる。



記号の説明

K1A　接触器

SW1A　スイッチ

図 I.2－例 A の安全関連部を特定するための安全関連ブロックダイアグラム

I.3.2　各チャネルの $MTTF_d$，DC_{avg}，共通原因故障（CCF），カテゴリ，PL の定量化

各チャネルの $MTTF_d$，DC_{avg}，及び共通原因故障の値は，**附属書 C**，**附属書 D**，及び**附属書 F** に従って見積る，又は製造業者によって示されることを仮定している。カテゴリは，**6.2** に従って見積る。

－　$MTTF_d$

接触器 K1A 及びスイッチ SW1A は，当該単一チャネルの $MTTF_d$ に寄与する。$MTTF_{d,K1A}$＝50 年及び $MTTF_{d,SW1A}$＝20 年は，製造業者によって示されることを仮定している。**D.1** のパーツ・カウント・メソッドによって，1 チャネルの $MTTF_d$ が明らかになる。

$$\frac{1}{MTTF_d}+\frac{1}{MTTF_{SW1A}}+\frac{1}{MTTF_{K1A}}=\frac{1}{20\text{年}}+\frac{1}{50\text{年}}=\frac{0.07}{\text{年}} \qquad \text{(I.1)}$$

上の式(I.1)から，$MTTF_d$＝14.3 年，又は **4.5.2**，**表 5** からそのチャネルは“中”が導き出される。

注記　K1A に関して利用可能な情報がない場合，**C.2** 又は **C.4** に従って最悪ケースを想定する。

－　DC（診断範囲）

制御回路 A では機能試験は不在なので，**4.5.3**，**表 6** に従って，DC＝0，又は“なし”となる。

－　カテゴリ

この回路の推奨カテゴリは，カテゴリ 1 であるが，チャネルの $MTTF_d$ は“中”である。このことは，この設計ではカテゴリ B だけが達成されることを意味する。

図 5 に対する入力データ：各チャネルの $MTTF_d$ は，“中”（14.3 年），DC_{avg} は“なし”，及びカテゴリは B である。

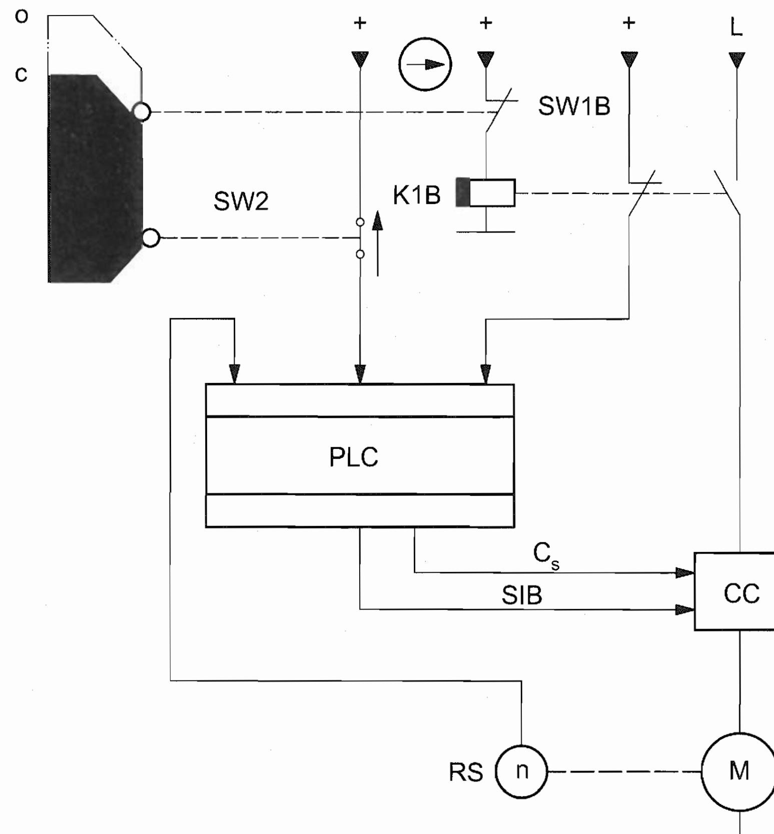
これは，パフォーマンスレベル PL＝b と解釈される。

この結果は，**I.2** による要求パフォーマンスレベル PL＝c と整合しない。よって，この回路は，**I.2** の適用例のリスク低減の要求事項を満たすために，パフォーマンスレベル PL＝c が達成されるまで再設計及び再評価しなければならない。

I.4　例 B，冗長システム

I.4.1　安全関連部の特定

安全機能に寄与する全てのコンポーネントは，**図 I.3** で示される。インタロックの安全機能（起動及び停止スイッチ又は K1B の遅れスイッチとして）に寄与しない機能の詳細は，省略してある。



記号の説明

PLC	プログラマブルロジックコントローラ	C_s	停止機能（標準）
CC	電流変換器	SIB	安全パルスのブロッキング
M	モータ	K1B	接触器
RS	回転センサ	SW1B	スイッチ（ノーマルクローズ）
o	開	SW2	スイッチ（ノーマルオープン）
c	閉	+	直流電源
		L	交流電源

図 I.3－安全機能を遂行する制御回路 B

この第 2 の例では，冗長系を提供するために，2 チャネルが用いられている。第 1 チャネルは，例 A と類似のものであり，直接開離作用のドアスイッチを用いて，かつ，ポジティブモードの作動で構成されている。このドアスイッチはモータへの電源を遮断できる接触器に接続されている。第 2 チャネルでは，追加の（プログラマブル）電子式コンポーネントが使用される。第 2 のドアスイッチは，プログラマブルロジックコントローラ（PLC）に接続されていて，コントローラはモータへの電源を遮断するための電流変換器を制御することができる。

次のように構成される。

－ 冗長チャネルであり，一つが電気機械式であり，もう一つはプログラマブル電子式である。

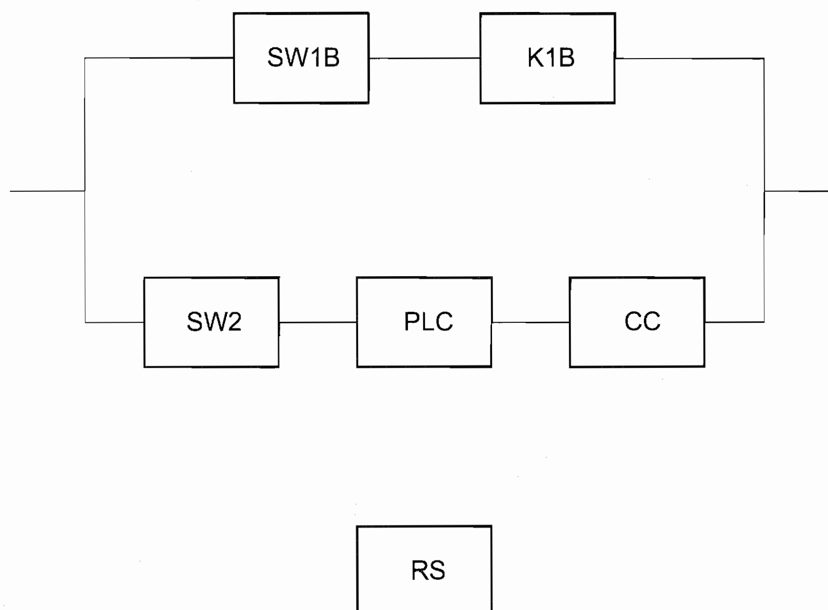
－ スイッチ SW1B は，ポジティブな機械的作用の接点をもち，SW2 は，$MTTF_d$＝“中”である。

－ 接触器 K1B は，$MTTF_d$＝“中”であり，この例で選択の接触器は，“十分吟味された”コンポーネントではない。

－ 電子式コンポーネントは，$MTTF_d$＝“中”である。

安全関連部及びその各チャネルへの分割は，**図 I.4** で示される安全関連部ブロックダイアグラムで示すことができる。

注記 冗長多様性（ダイバーシティ）に関しては，PLC 経路に対する **4.6** によるソフトウェアの要求事項は，関連するものとして考慮しない。



SW1B 及び K1B は，第 1 のチャネルを構成し，SW2，PLC 及び CC は，第 2 チャネルを構成する。RS は，電流変換器を試験するためにだけ使用される。

記号の説明

SW1B　インタロック装置
K1B　接触器
SW2　スイッチ
PLC　プログラマブルロジックコントローラ
CC　電流変換器
RS　回転センサ

図 I.4－例 B の安全関連部を特定するためのブロックダイアグラム

I.4.2　各チャネルの $\mathbf{MTTF_d}$，$\mathbf{DC_{avg}}$，共通原因故障（CCF），カテゴリ及び PL の定量化

各チャネルの $MTTF_d$，DC_{avg} 及び共通原因故障の値は，**附属書 C**，**附属書 D**，**附属書 E** 及び**附属書 F** に従って見積りされる，又は製造業者によって示されることを仮定している。カテゴリは，**6.2** によって見積りされる。

スイッチ SW1B は，直接開離の作用をもち，かつ，ポジティブモードの作動で使用される。したがって，障害の除外が，機械的故障（例えば，プランジャーの破損，作用カムの摩耗，調整不良）による接点の非開放及びスイッチの不作動に関係してなされる。

注記 これらの仮定は，**JIS C 8201-5-1** の**附属書 K** に従った補助回路スイッチ，及び製造業者の仕様書（**ISO 13849-2** 参照）に従ったスイッチの適切な機械的固定及び作動について有効である。

－　$MTTF_d$

接触器 K1B は，第 1 チャネルの $MTTF_d$ に寄与する唯一のコンポーネントである。製造業者によって示されて，$MTTF_{K1B}$ は，30 年が仮定される。**D.1** のパーツ・カウント・メソッドによって，第 1 チ

ャネルの $MTTF_d$ が明らかになる。

$$\frac{1}{MTTF_{dC1}}+\frac{1}{MTTF_{dK1B}} \quad \text{(I.2)}$$

式(I.2)から，第 1 チャネルの $MTTF_d$＝30 年が導き出される。

第 2 チャネルにおいて，SW2，PLC 及び CC は $MTTF_{dC2}$ に寄与している。この三つのコンポーネントは，RS と同様に，製造業者によって $MTTF_d$＝20 年が示されることを仮定している。**D.1** のパーツ・カウント・メソッドによって，第 2 チャネルの $MTTF_{dC2}$ が明らかになる。

$$\frac{1}{MTTF_{dC2}}+\frac{1}{MTTF_{dSW2}}+\frac{1}{MTTF_{dPLC}}+\frac{1}{MTTF_{dCC}}=\frac{1}{20\text{年}}+\frac{1}{20\text{年}}+\frac{1}{20\text{年}}=\frac{0.15}{\text{年}} \quad \text{(I.3)}$$

式(I.3)から第 2 チャネルの $MTTF_d$＝6.7 年が導き出される。

両方のチャネルは，互いに異なる $MTTF_d$ をもつので，対称 2 チャネルシステムの単一チャネルに対する $MTTF_d$ 代用値を計算するために **D.2** の式(D.2)を使用することができる。式(D.2)は，$MTTF_d$＝20 年又は **4.5.2** の**表 5** に従い“中”であることが明らかになる。

－ DC

制御回路 B では，安全関連部のうちの四つが PLC によって試験される。すなわち，SW2 及び K1B は，PLC によってリードバックされ，PLC が自己試験を実施し，かつ，CC も RS を経由して PLC にリードバックされる。試験される全ての部分に関連する DC は，次のとおりである。

1) DC_{sw2}＝60 %，“低”であり，動的試験なしの入力信号の監視による。**表 E.1** 参照（入力装置の EI-3）。

2) DC_{K1B}＝99 %，“高”であり，ノーマルオープン及びノーマルクローズの機械的結合の接点による。**表 E.1** 参照（入力装置部の EI-2）。

3) DC_{PLC}＝30 %，“なし”であり，自己試験の低有効性による（製造業者が，FMEA によってこの値を計算したことを仮定している）。

4) DC_{CC}＝90 %，“中”であり，制御論理によるアクチュエータ監視をもつ冗長なシャットダウンパスによる。**表 E.1** 参照（出力装置の EO-6）。PLC が CC の故障を監視する場合，安全パルスのブロッキング（追加のシャットダウンパス）によって動きを停止させることができる。

PL の見積りに対して，**図 5** の入力として平均 DC 値（DC_{avg}）が必要となる。

$$DC_{avg}=\frac{\frac{DC_{SW2}}{MTTF_{dSW2}}+\frac{DC_{K1B}}{MTTF_{dK1B}}+\frac{DC_{PLC}}{MTTF_{dPLC}}+\frac{DC_{CC}}{MTTF_{dCC}}}{\frac{1}{MTTF_{dSW2}}+\frac{1}{MTTF_{dK1B}}+\frac{1}{MTTF_{dPLC}}+\frac{1}{MTTF_{dCC}}}$$

$$=\frac{\frac{0.6}{20\text{年}}+\frac{0.99}{30\text{年}}+\frac{0.3}{20\text{年}}+\frac{0.9}{20\text{年}}}{\frac{1}{20\text{年}}+\frac{1}{30\text{年}}+\frac{1}{20\text{年}}+\frac{1}{20\text{年}}}=\frac{0.123}{0.183}=67.1\,\% \quad \text{(I.4)}$$

よって，DC_{avg} は，**4.5.3** 及び**表 6** に従って“低”となる。

－ CCF

F.2 に従って，CCF に対する方策の見積りは，制御回路 B に対して実施されたことを仮定している。スコアは，**表 I.1** に示すように主張される。

表 I.1－例 B に対する CCF 対策の見積り

No	アイテム	制御回路のスコア	最大可能スコア
1	分離／隔離		
	信号経路間の物理的な分離	15	15
2	多様性（ダイバーシティ）		
	異なる技術的方式／設計又は物理的原理を用いているか？	20	20
3	設計／適用／経験		
3.1	過電圧，過圧，過電流などに対する保護	なし	15
3.2	使用のコンポーネントは十分吟味されている。	5	5
4	査定／分析		
	設計上での共通原因故障を回避するために，FMEA の結果を考慮しているか？	5	5
5	適格性（能力）／訓練		
	設計者は，共通原因故障に対して原因及び結果を理解できるように訓練されているか？	なし	5
6	環境面		
6.1	適切な規格に従った CCF 対応の汚染防止及び電磁両立性（EMC）の防止	25	25
6.2	他の影響 温度，衝撃，振動，湿度（例えば，関連の規格で規定されるように）のような環境関連の影響の全てに対してイミュニティの要求事項を考慮しているか？	10	10
	合計	80	最大　100

CCF に対する十分な方策には，最低のスコア 65 が必要である。例 B では，スコア 80 は CCF に対する要求事項を満たす。

制御回路のいずれかの部分での単一障害は，安全機能の喪失にはつながらない。合理的に実施可能な場合，単一障害は，安全機能に対する次の動作要求時又はその前に検出される。診断範囲（DC）は，60 %～90 %までの範囲にある。CCF に対する方策は，十分である。これらの特性は，カテゴリ 3 の代表的例である。

図 5 に対する入力データ：チャネルの $MTTF_d$ は，“中”（20 年）であり，DC_{avg} は，“低”で，かつ，カテゴリは，3 である。

これによって，パフォーマンスレベル c として解釈できる。

この結果は，**I.2** の要求パフォーマンスレベル PLc に適合する。よって，制御回路 B は，**I.2** の適用例のリスク低減の要求事項を満たす。

附属書 J
（参考）
ソフトウェア

J.1　事例の記述

この附属書は，要求パフォーマンスレベル $PL_r=d$ における制御システムの安全関連部（SRP/CS）の安全関連組込みソフトウェア（SRESW）実現のための模範的な活動を提示する。SRP/CS は，機械装置に連結され，次を保証する。

－　種々のセンサによって送られる取得情報

－　安全要求事項を考慮に入れながら制御要素の操作が求められる処理

－　アクチュエータの制御

ファンクションブロックレベル上でのこの適用の SRESW の設計は，**図 J.1** に示すとおりである。

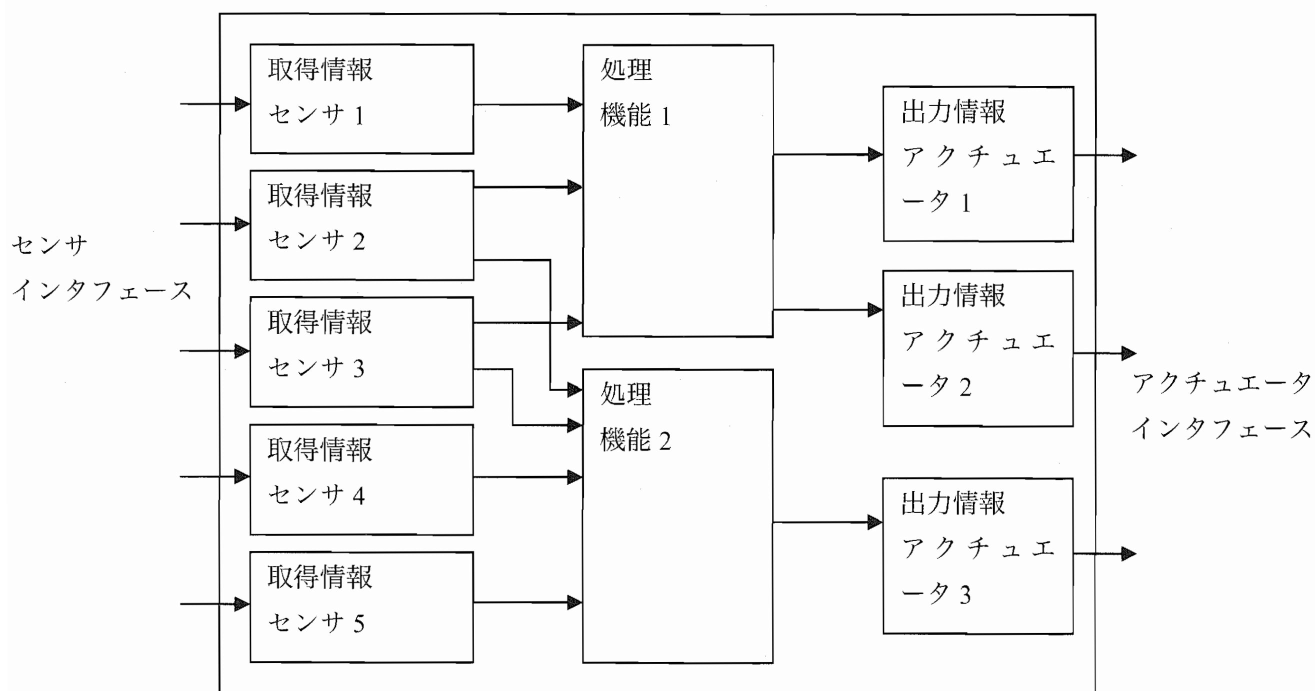


図 J.1－ソフトウェアのファンクションブロックレベルでの設計の事例

J.2　ソフトウェア安全ライフサイクルの V モデルへの適用

表 J.1 は，機械制御のためのソフトウェア安全ライフサイクルの V モデルへの適用における総合的な活動及び文書を模範的に示す。

表 J.1－ソフトウェア安全ライフサイクルにおける活動及び文書

開発活動	検証活動	関連する文書
機械の側面： SRP/CS に関わる機能の同定	安全関連機能の同定	“機械制御のための安全関連仕様”
アーキテクチャの側面： センサ及びアクチュエータの制御アーキテクチャの定義	選択するコンポーネントの安全特性に関するコメント	“制御アーキテクチャの定義”
ソフトウェア仕様の側面： ソフトウェア機能への機械機能の転写	記述の再読（**J.3** 参照）	“ソフトウェアの記述”
ソフトウェアアーキテクチャの側面： ファンクションブロックで機能を詳細に。	より大きい見直しの主題及び妥当性確認の努力などの重要なブロックの定義	“ファンクションブロックのモデリング”
符号化の側面： プログラミング規則に従う符号化（**J.4** 参照）	コードの再読。機能の検証及び規則への適合	“コード中のコメントの符号化” “再読シートの符号化”
妥当性確認の側面： 試験シナリオの作成： 機能の操作側面 失敗における挙動側面	試験範囲の検証 試験結果の検証	相互参照仕様パラグラフと試験の“対応行列” 試験シナリオ及び獲得した結果のコメントを包括した“試験シート”

J.3　ソフトウェア仕様の検証

ソフトウェア安全ライフサイクルの一部として，ソフトウェア仕様レベルにおける検証活動には，細心の注意を払う必要がある全てのポイントが正しく記述されていることの検討が含まれる。各機能を検証するときは，次を考慮することが望ましい。

－　システム仕様に関して誤りの解釈が生じた場合の制限
－　制御システムの安全関連部（SRP/CS）の先天的な未知の挙動でもたらされる仕様上の欠落の回避
－　機能の活性化（起動）及び不活性化（非起動）の条件の正確な定義
－　可能な全てのケースが処理されることの正確な保証
－　一貫性テスト
－　異なるパラメータ化の場合
－　故障時に引き続いて起こる反応

J.4　プログラミング規則の事例

共通原因故障（CCF）に対して，一般に，作者によるプログラム，ロード年月日，バージョン及びアクセスの最後の種類の信ぴょう性確認を可能にすることが望ましい。プログラミング規則に関して，次の規則で区別することが可能である。

a) **プログラム構造レベルでのプログラミング規則**　異なる処理を容易に局所化し，一貫して，かつ，理解できる一般的な骨組みを表すためにプログラミングを構造化することが望ましい。これには，次を含む。

1) 代表的なプログラム又はファンクションブロック用のテンプレート（定規）の使用

2) “入力”，“処理”，及び“出力”に対応する主要部分を同定するために，セグメントでのプログラムの分割

3) 変更の場合には，コメントのアップデートを容易にするために，プログラムソース中の各プログラ

ム部分のコメント

4) ファンクションブロックが呼ばれた時に果たす役割の記述

5) メモリ領域は単一種のデータ形だけによって使用されて，かつ，ユニークなラベルによって印されることが望ましい。かつ，

6) 動作シーケンスは，プログラムの実行時に計算されるジャンプアドレスのような変数に依存するのではなく，条件付きジャンプによって権限が付与されることが望ましい。

b) **変数の使用に関するプログラミング規則**

- 全ての出力の活性化（起動）又は不活性化（非起動）は，1 か所だけで行われることが望ましい（条件の集中化）
- 変数をアップデートするための式は，集中化されるように構造化することが望ましい。
- 入力又は出力の各グローバル変数は，ニューモニック・ネームにして十分に明白にし，かつ，ソース中のコメントで説明することが望ましい。

c) **ファンクションブロックレベルでのプログラミング規則**

- 望ましくは，制御システムの安全関連部（SRP/CS）の供給者によって妥当性を確認されたファンクションブロックを使用し，プログラムの状態に対応するこれらの妥当性を確認されたブロックに対して想定される運転条件をチェックする。
- コード化されたブロックの大きさは，次の指針値に制限することが望ましい。
  1) パラメータ：最大 8 デジタル及び二つの整数の入力，一つの出力
  2) 機能コード：最大 10 のローカル変数，最大 20 のブーリアン方程式
- ファンクションブロックでグローバル変数の変更はしないほうがよい。
- デジタル値は，正当性の領域を保証するためにプリセットベンチマークに関連して制御することが望ましい。
- ファンクションブロックは，処理される変数の不一致を検出することが望ましい。
- 1 ブロックの障害コードは，一つの障害を他から識別するのにアクセスしやすくすることが望ましい。
- 障害検出後の障害コード及びブロックの状況は，コメントで説明することが望ましい。
- ブロックのリセット又は正規の状態への回復は，コメントで説明することが望ましい。

附属書 K
（参考）
図 5 の数値

図 5 における MTTF$_d$，DC，カテゴリ及び PL は，**表 K.1** を参照。

表 K.1－図 5 の数値

各チャネルの $MTTF_d$ 年	危険側故障の平均確率（1/h）及び対応のパフォーマンスレベル PL						
	カテゴリ B PL DC_{avg}＝“なし”	カテゴリ 1 PL DC_{avg}＝“なし”	カテゴリ 2 PL DC_{avg}＝“低”	カテゴリ 2 PL DC_{avg}＝“中”	カテゴリ 3 PL DC_{avg}＝“低”	カテゴリ 3 PL DC_{avg}＝“中”	カテゴリ 4 PL DC_{avg}＝“高”
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
3.3	3.46×10^{-5} a		2.33×10^{-5} a	1.79×10^{-5} a	1.13×10^{-5} a	5.41×10^{-6} b	
3.6	3.17×10^{-5} a		2.13×10^{-5} a	1.62×10^{-5} a	1.03×10^{-5} a	4.86×10^{-6} b	
3.9	2.93×10^{-5} a		1.95×10^{-5} a	1.48×10^{-5} a	9.37×10^{-6} b	4.40×10^{-6} b	
4.3	2.65×10^{-5} a		1.76×10^{-5} a	1.33×10^{-5} a	8.39×10^{-6} b	3.89×10^{-6} b	
4.7	2.43×10^{-5} a		1.60×10^{-5} a	1.20×10^{-5} a	7.58×10^{-6} b	3.48×10^{-6} b	
5.1	2.24×10^{-5} a		1.47×10^{-5} a	1.10×10^{-5} a	6.91×10^{-6} b	3.15×10^{-6} b	
5.6	2.04×10^{-5} a		1.33×10^{-5} a	9.87×10^{-6} b	6.21×10^{-6} b	2.80×10^{-6} c	
6.2	1.84×10^{-5} a		1.19×10^{-5} a	8.80×10^{-6} b	5.53×10^{-6} b	2.47×10^{-6} c	
6.8	1.68×10^{-5} a		1.08×10^{-5} a	7.93×10^{-6} b	4.98×10^{-6} b	2.20×10^{-6} c	
7.5	1.52×10^{-5} a		9.75×10^{-6} b	7.10×10^{-6} b	4.45×10^{-6} b	1.95×10^{-6} c	
8.2	1.39×10^{-5} a		8.87×10^{-6} b	6.43×10^{-6} b	4.02×10^{-6} b	1.74×10^{-6} c	
9.1	1.25×10^{-5} a		7.94×10^{-6} b	5.71×10^{-6} b	3.57×10^{-6} b	1.53×10^{-6} c	
10	1.14×10^{-5} a		7.18×10^{-6} b	5.14×10^{-6} b	3.21×10^{-6} b	1.36×10^{-6} c	
11	1.04×10^{-5} a		6.44×10^{-6} b	4.53×10^{-6} b	2.81×10^{-6} c	1.18×10^{-6} c	
12	9.51×10^{-6} b		5.84×10^{-6} b	4.04×10^{-6} b	2.49×10^{-6} c	1.04×10^{-6} c	
13	8.78×10^{-6} b		5.33×10^{-6} b	3.64×10^{-6} b	2.23×10^{-6} c	9.21×10^{-7} d	
15	7.61×10^{-6} b		4.53×10^{-6} b	3.01×10^{-6} b	1.82×10^{-6} c	7.44×10^{-7} d	
16	7.13×10^{-6} b		4.21×10^{-6} b	2.77×10^{-6} c	1.67×10^{-6} c	6.76×10^{-7} d	
18	6.34×10^{-6} b		3.68×10^{-6} b	2.37×10^{-6} c	1.41×10^{-6} c	5.67×10^{-7} d	
20	5.71×10^{-6} b		3.26×10^{-6} b	2.06×10^{-6} c	1.22×10^{-6} c	4.85×10^{-7} d	
22	5.19×10^{-6} b		2.93×10^{-6} c	1.82×10^{-6} c	1.07×10^{-6} c	4.21×10^{-7} d	
24	4.76×10^{-6} b		2.65×10^{-6} c	1.62×10^{-6} c	9.47×10^{-7} d	3.70×10^{-7} d	
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e

表 K.1－図 5 の数値（続き）

各チャネルの $MTTF_d$ 年	危険側故障の平均確率（1/h）及び対応のパフォーマンスレベル PL						
	カテゴリ B　PL DC_{avg}＝“なし”	カテゴリ 1　PL DC_{avg}＝“なし”	カテゴリ 2　PL DC_{avg}＝“低”	カテゴリ 2　PL DC_{avg}＝“中”	カテゴリ 3　PL DC_{avg}＝“低”	カテゴリ 3　PL DC_{avg}＝“中”	カテゴリ 4　PL DC_{avg}＝“高”
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51		2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56		2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62		1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e
68		1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75		1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e
82		1.39×10^{-6} c	6.61×10^{-7} d	3.01×10^{-7} d	1.35×10^{-7} d	5.79×10^{-8} e	3.08×10^{-8} e
91		1.25×10^{-6} c	5.88×10^{-7} d	2.61×10^{-7} d	1.14×10^{-7} d	4.94×10^{-8} e	2.74×10^{-8} e
100		1.14×10^{-6} c	5.28×10^{-7} d	2.29×10^{-7} d	1.01×10^{-7} d	4.29×10^{-8} e	2.47×10^{-8} e

参考文献

1　プログラマブル電子システムに関する文献

[1]　**JIS C 61000-4-4**　電磁両立性－第 4-4 部：試験及び測定技術－電気的ファストトランジェント／バーストイミュニティ試験

注記　対応国際規格：**IEC 61000-4-4**，Electromagnetic compatibility (EMC)－Part 4-4: Testing and measurement techniques－Electrical fast transient/burst immunity test（IDT）

[2]　**JIS B 9704-1**　機械類の安全性－電気的検知保護設備－第 1 部：一般要求事項及び試験

注記　対応国際規格：**IEC 61496-1**，Safety of machinery－Electro-sensitive protective equipment－Part 1: General requirements and tests（IDT）

[3]　**JIS B 9704-2**　機械類の安全性－電気的検知保護設備－第 2 部：能動的光電保護装置を使う設備に対する要求事項

注記　対応国際規格：**IEC 61496-2**，Safety of machinery－Electro-sensitive protective equipment－Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs)（IDT）

[4]　**JIS B 9704-3**　機械類の安全性－電気的検知保護設備－第 3 部：拡散反射形能動的光電保護装置に対する要求事項

注記　対応国際規格：**IEC 61496-3**，Safety of machinery－Electro-sensitive protective equipment－Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)（IDT）

[5]　**JIS B 9717-1**　機械類の安全性－圧力検知保護装置－第 1 部：圧力検知マット及び圧力検知フロアの設計及び試験のための一般原則

注記　対応国際規格：**ISO 13856-1**，Safety of machinery－Pressure-sensitive protective devices－Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors（IDT）

[6]　**JIS B 9961**:2008　機械類の安全性－安全関連の電気・電子・プログラマブル電子制御システムの機能安全

注記　対応国際規格：**IEC 62061**:2005，Safety of machinery－Functional safety of safety-related electrical, electronic and programmable electronic control systems（IDT）

[7]　**IEC 61508-1**:1998，Functional safety of electrical/electronic/programmable electronic safety-related systems－Part 1: General requirements

[8]　**IEC 61508-2**:2000，Functional safety of electrical/electronic/programmable electronic safety-related systems－Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[9]　**IEC 61508-5**:1998，Functional safety of electrical/electronic/programmable electronic safety related systems－Part 5: Examples of methods for the determination of safety integrity levels

[10]　**IEC 61508-6**:2000，Functional safety of electrical/electronic/programmable electronic safety-related systems－Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

[11]　**IEC 61508-7**:2000，Functional safety of electrical/electronic/programmable electronic safety-related systems－Part 7: Overview of techniques and measures

[12] **IEC 61511-1**, Functional safety－Safety instrumented systems for the process industry sector－Part 1: Framework, definitions, system, hardware and software requirements

[13] **HSE** Guidelines, Programmable Electronic Systems in Safety-related Applications, Parts 1 (ISBN 0 11 883906 6) and 2 (ISBN 0 11 883906 3)

[14] **CECR-184**, Personal Safety in Microprocessor Control Systems (Elektronikcentralen, Denmark)

2 他の文献

[15] **JIS B 9703** 機械類の安全性－非常停止－設計原則

注記 対応国際規格：**ISO 13850**, Safety of machinery－Emergency stop－Principles for design（IDT）

[16] **JIS B 9706**（規格群） 機械類の安全性－表示，マーキング及び操作

注記 対応国際規格：**IEC 61310** (all parts), Safety of machinery－Indication, marking and actuation（IDT）

[17] **JIS B 9710** 機械類の安全性－ガードと共同するインタロック装置－設計及び選択のための原則

注記 対応国際規格：**ISO 14119**, Safety of machinery－Interlocking devices associated with guards－Principles for design and selection（IDT）

[18] **JIS B 9712** 機械類の安全性－両手操作制御装置－機能的側面及び設計原則

注記 対応国際規格：**ISO 13851**, Safety of machinery－Two-hand control devices－Functional aspects and design principles（IDT）

[19] **JIS B 9714** 機械類の安全性－予期しない起動の防止

注記 対応国際規格：**ISO 14118**, Safety of machinery－Prevention of unexpected start-up（IDT）

[20] **JIS B 9715** 機械類の安全性－人体部位の接近速度に基づく保護設備の位置決め

注記 対応国際規格：**ISO 13855**:2000, Safety of machinery－Positioning of protective equipment with respect to the approach speeds of parts of the human body（IDT）

[21] **JIS B 9960-1** 機械類の安全性－機械の電気装置－第1部：一般要求事項

注記 対応国際規格：**IEC 60204-1**, Safety of machinery－Electrical equipment of machines－Part 1: General requirements（MOD）

[22] **JIS C 4421** 可変速駆動システム（PDS）－電磁両立性（EMC）要求事項及び試験方法

注記 対応国際規格：**IEC 61800-3**, Adjustable speed electrical power drive systems－Part 3: EMC requirements and specific test methods（MOD）

[23] **JIS C 8201**（規格群）低圧開閉装置及び制御装置

注記 対応国際規格：**IEC 60947** (all parts), Low-voltage switchgear and controlgear（MOD）

[24] **JIS C 61000-6-2** 電磁両立性－第6-2部：共通規格－工業環境におけるイミュニティ

注記 対応国際規格：**IEC 61000-6-2**, Electromagnetic compatibility (EMC)－Part 6-2: Generic standards－Immunity for industrial environments（MOD）

[25] **JIS Q 9001** 品質マネジメントシステム－要求事項

注記 対応国際規格：**ISO 9001**, Quality management systems－Requirements（IDT）

[26] **JIS B 8361**:2000 油圧システム通則

注記 対応国際規格：**ISO 4413**, Hydraulic fluid power－General rules relating to systems（IDT）

[27] **JIS B 8370**:2000 空気圧システム通則

注記 対応国際規格：**ISO 4414**, Pneumatic fluid power－General rules relating to systems（IDT）

[28] **JIS C 0920**　電気機械器具の外郭による保護等級（IP コード）
　　注記　対応国際規格：**IEC 60529**，Degrees of protection provided by enclosures (IP code)（IDT）

[29] **ISO 13856-2**，Safety of machinery－Pressure-sensitive protective devices－Part 2: General principles for the design and testing of pressure-sensitive edges and pressure-sensitive bars

[30] **ISO 11428**，Ergonomics－Visual danger signals－General requirements, design and testing

[31] **ISO 9355-1**，Ergonomic requirements for the design of displays and control actuators－Part 1: Human interactions with displays and control actuators

[32] **ISO 9355-2**，Ergonomic requirements for the design of displays and control actuators－Part 2: Displays

[33] **ISO 9355-3**，Ergonomic requirements for the design of displays and control actuators－Part 3: Control actuators

[34] **ISO 11429**，Ergonomics－System of auditory and visual danger and information signals

[35] **ISO 7731**，Ergonomics－Danger signals for public and work areas－Auditory danger signals

[36] **ISO 19973** (all parts)，Pneumatic fluid power－Assessment of component reliability by testing

[37] **IEC 60447**，Basic and safety principles for man-machine interface, marking and identification－Actuating principles

[38] **IEC 60812**，Analysis techniques for system reliability－Procedure for failure mode and effects analysis (FMEA)

[39] **IEC 61810** (all parts)，Electromechanical elementary relays

[40] **IEC 61300** (all parts)，Fibre optic interconnecting devices and passive components－Basic test and measurement procedures

[41] **JIS B 3503**　プログラマブルコントローラ－プログラム言語
　　注記　対応国際規格：**IEC 61131-3**，Programmable controllers－Part 3: Programming languages（IDT）

[42] **IEC 61131** (all parts)，Programmable controllers

[43] **EN 457**，Safety of machinery. Auditory danger signals. General requirements, design and testing

[44] **EN 614-1**，Safety of machinery－Ergonomic design principles－Part 1: Terminology and general principles

[45] **EN 982**，Safety of machinery. Safety requirements for fluid power systems and their components. Hydraulics

[46] **EN 983**，Safety of machinery. Safety requirements for fluid power systems and their components. Pneumatics

[47] **EN 1005-3**，Safety of machinery－Human physical performance－Part 3: Recommended force limits for machinery operation

[48] **EN 50205**，Relays with forcibly guided (mechanically linked) contacts

[49] **SN 29500** (all parts)，Failure rates of components

[50] GOBLE, W.M. Control systems－Evaluation and Reliability. 2nd Edition. Instrument Society of America (ISA), North Carolina, 1998

3　データベース

[51] **SN 29500**，Failure rates of components, Edition 1999-11, Siemens AG 1999, www.pruefinstitut.de

[52] **IEC/TR 62380**，Reliability data handbook－Universal model for reliability prediction of electronics components, PCBs and equipment, identical to RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l'Electricité et de la Communication (www.ute-fr.com)

[53] Reliability Prediction of Electronic Equipment, **MIL-HDBK-217E**, Department of Defense, Washington DC,

1982

[54] Reliability Prediction Procedure for Electronic Equipment, Telcordia SR-332, Issue 01, May 2001(telecom-info.telcordia.com), Bellcore TR-332, Issue 06

[55] EPRD, Electronic Parts Reliability Data (**RAC-STD-6100**), Reliability Analysis Centre, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)

[56] **NPRD-95**, Non-electronic Parts Reliability Data (**RAC-STD-6200**), Reliability Analysis Centre, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)

[57] British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)

[58] Chinese Military Standard, **GJB/z 299B**

JIS B 9705-1：2011
(ISO 13849-1：2006)
機械類の安全性－制御システムの安全関連部－第1部：設計のための一般原則
解　説

この解説は，規格に規定・記載した事柄を説明するもので，規格の一部ではない。

この解説は，財団法人日本規格協会が編集・発行するものであり，これに関する問合せ先は，財団法人日本規格協会である。

1　今回の改正までの経緯

この規格は，欧州機械である **EN 954-1** をウィーン協定に基づいて発行された **ISO 13849-1**:1999 の完全一致規格として制定（以下，旧規格という。）された後，今回の改正に至った。

今回，社団法人日本機械工業連合会は，**JIS** 原案作成委員会を組織し，**JIS** 原案を作成した。この **JIS** 原案を主務大臣である厚生労働大臣及び経済産業大臣に申出し，日本工業標準調査会で審議議決され，平成23年7月25日付で公示された。

2　今回の改正の趣旨

旧規格は，**ISO 13849-1**:1999, Safety of machinery－Safety-related parts of control systems－Part 1: General principles for design の国際一致規格であった。2006年11月に **ISO 13849-1**:2006 (Ed.2) が発行されたので，この規格を **ISO 13849-1**:2006 に整合させることを目的に，一致規格（IDT）として改正を行った。

なお，**ISO 13849-1**:2006 は，ISO/TC199（機械類の安全性）とミラーの関係にある CEN/TC114（機械類の安全性）リードで改定作業が進められたものである。

3　審議中に特に問題となった事項

今回のこの規格の改正審議で問題となった主な事項は，次のとおりである。

a)　**信頼性データ適用の問題**　信頼性データの適用について**附属書 C** は **SN 29500** から抽出されたものであるが，設計者がコンポーネントに対して信頼できるほかのデータをもっている場合は，そのデータの使用が推奨されているが，データの評価基準は明確でない。信頼性データはむしろ将来変化しやすい状況にあり，扱うデータはあまりにも確実性に不足していると思われる。

　特に安全方策が信頼性だけに依存する場合，まず，信頼性データ自体の立証の難しさ及びデータの改ざんを考慮すべきである。信頼性データの立証問題は，データ自体の運用条件及び環境条件が必ずしも明示されないままに（又は比較なしに）適用されるおそれがある。参考として **JIS B 9702**:2000 の **8.3** では機械類に関してリスク比較の基準を，次のように示している。

－　その類似機械類が安全である。
－　意図する使用及び使用法が，双方の機械で比較可能である。
－　危険源及びリスク要素が比較可能である。

－　技術的仕様が比較可能である。

－　使用条件が比較可能である。

4　規定項目の内容

4.1　適用範囲（箇条 1）

要求されるリスク低減方策には，機械自体に存在する角部などの危険部位を除去したり，作業者の筋負担を軽減したり，危険な可動部分を監視できるように視認性を確保するような方法と，意図しない機械の起動，無制御状態の速度変化，運動部分の停止不能，保護装置の機能停止などを生じないように機械の制御システムにより安全性を確保する方法がある。別の言い方をすれば，保護方策が制御システムに依存する場合と依存しない場合とが考えられるが，この選択については，リスクアセスメントに基づいて，決定されることとなる。

この規格では，リスク低減が制御システムに依存する場合の制御システムの安全関連部の設計方策が規定される。制御システムには，安全に関わる部分＝制御システムの安全関連部と，安全にかかわらない部分＝非制御システム安全関連部がある。この規格では，**図 3** に示すステップで制御システムの安全関連部を設計することが規定される。

なお，類似の規格として **JIS B 9961** があるが，この規格との使い分けについては，**表 1** に示されている。また，これら二つの規格の使用ガイダンスとして，**ISO/TR 23849**:2010，Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery が発行されている。

4.2　用語

4.2.1　“3.1.1　制御システムの安全関連部”　入力信号に応じて安全に関わる出力信号を生成するような制御システムの部分を指す。

4.2.2　“フォールト・レジスタンス”　例えば，制御システムに故障が生じた場合，たとえ制御機能を失っても，安全機能は失わない機能を意味する。安全性確保に対する抵抗性を意味している。

4.2.3　“フォールト・トレランス”　例えば，制御システムに故障が生じた場合，その制御機能を達成し，かつ，維持するような技術的手法を意味する。

4.2.4　“グッド・エンジニアリング・プラクティス”　この規格においては，優れた工学上の取組みやその事例のことを示す。

4.2.5　“3.1.3　障害”　**JIS B 9700-1**:2004 では，不具合（障害）としているが，この規格では“障害”とした。

4.2.6　“十分吟味された”　この規格では“十分吟味された”安全原則，“十分吟味された”コンポーネントのように，特殊用語として“十分吟味された”が使用されている。対応国際規格では，“Well-tried”と表現されており，これは，単に信頼性が高いことだけを意味するものではない。“十分吟味された”を満たす条件を，次に示す。

a)　類似の用途において，好結果で過去に広く使用されたこと（使用実績がある）。

b)　安全関連への用途に対して適切性及び信頼性を論証するための原則を用いて製作され，かつ，検証されたこと。

4.2.7　“should”　旧規格では，“should”を“すべき”としたが，**JIS Z 8301** においては，“すべき”を使用することはできないので，“することが望ましい”，“するのがよい”とした。しかし，この規格は安全性に関するものであり，“～するとよい”と訳しても，推奨より強い意味をもつことに注意が必要である。

4.3　“6.2.3 カテゴリ B～6.2.7 カテゴリ 4”

4.3.1　“6.2.3　カテゴリ B”

通常の制御システムとしての機能を所有する状態を意味しており，安全機能として次のカテゴリ 1 からカテゴリ 4 で示すような配慮がなされていないような安全関連部の状態を意味している。

4.3.2　“6.2.4　カテゴリ 1”

十分吟味されたコンポーネントと十分吟味された安全原則を利用して構成された安全関連部である。十分吟味されたコンポーネントとは，電気部品であるならば，例えば，ヒューズや十分に絶縁されたトランスである。機能的構造であれば，例えば，頑丈に作られたガードとその周辺要素がそれに当たる。十分吟味された安全原則とは，電気的絶縁処理を二重化したり，電極間間隔を十分大きくして電極間短絡が生じないようにして，上述のヒューズやトランスを構成するような方法である。また，構成部品の結合にポジティブモードを利用して，上述のガード及びその周辺要素を構成するような方法である。

ただし，複雑な電子式コンポーネントは十分吟味されたコンポーネントとしては取り扱うことができないので，この規格の **6.2.4** の**注記 1** に示されるように，単一の電子式コンポーネントだけを用いてもカテゴリ 1 の安全関連部は実現できない。

4.3.3　“6.2.5　カテゴリ 2”

上述のカテゴリ 1 の要求事項を満たして，かつ，安全機能が適当な間隔でチェックされ，チェックの結果安全機能が果たされたいないとき，安全関連部の出力信号を停止するような機能をもつ安全関連部である。

4.3.4　“6.2.6　カテゴリ 3”

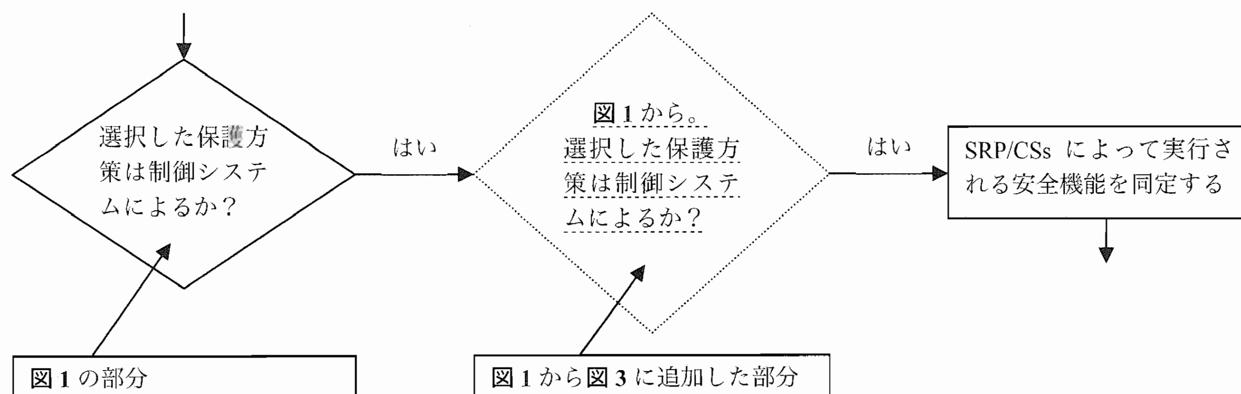
上述のカテゴリ 1 の要求事項を満たして，かつ，安全関連部を構成する要素のいずれか一つに障害が生じた場合，安全関連部の出力信号を停止するような機能をもつ安全関連部である。単一の障害を検出するために，2 チャンネルシステムがよく利用される。この場合，単純にカテゴリ 2 の安全関連部を用いて二重系にすればよいように見えるが，単一の障害検出には通常二重系の不一致検出を必要とする。この不一致検出にも，また単一の障害検出が必要であって，この障害が検出されたとき安全関連部の出力信号は停止することが必要である。

4.3.5　“6.2.7　カテゴリ 4”

上述のカテゴリ 1 の要求事項を満たして，かつ，安全関連部を構成する要素の単一の障害に対してカテゴリ 3 の出力特性をもつとともに，単一の障害を検出できない場合，障害の蓄積時に危険側の出力を生じないような特性をもつ安全関連部である。

4.4　“図 1”及び“図 3”の関係

図 1 及び**図 3** は，リスク低減のためのプロセスの概要と制御システムの安全関連部のプロセスが示されている。両図は互いに関係がある。対応国際規格の**図 3** の最初のブロック“SRP/CSs により実行される安全機能を同定する”の左からは，何も入力はないが，**図 1** と**図 3** の関係性を明示するために，**図 3** には，**図 1** の“選択した保護方策は制御システムによるか？”を追加した（**解説図 1** 参照）。



解説図 1－この規格の図 3 に追加した箇所

4.5　“グレイボックス試験”

ホワイトボックス試験とブラックボックス試験の中間に当たる試験である。

4.6　“V モデル”

ソフトウェア設計開発手法の一つで設計開発とそれに対応する試験で構成される。

5　その他解説事項

この規格では，解説の箇条 **4** で記述した“十分吟味された”安全原則及び“十分吟味された”コンポーネントが記載されている箇所がある。この例は，この規格の第 2 部（**ISO 13849-2**）：妥当性確認において記載されている事項である。参考までに，第 2 部で記載されている例を，**解説表 1**～**解説表 56** に示す。

a)　ISO 13849-2:2003，附属書 A（参考）機械システムの妥当性確認ツール

1)　基本安全原則一覧

解説表 1－基本安全原則

基本安全原則	注記
適した素材及び適切な製造方法の採用	次の要素を考慮した素材，製造方法，処理方法の選択。 －　応力，耐性，弾性，摩擦，磨耗，腐食，温度
正しい寸法及び形状の測定	次の要素を考慮すること。 －　応力，耐性，弾性，摩擦，磨耗，腐食，温度
適切な選択，組み合わせ，配置コンポーネント／システムの組立てと据付	製造者の適用ノート，例えば，カタログシート，据付説明書，仕様書，及び類似のコンポーネント／システムにおけるグッド・エンジニアリング・プラクティスなどを適用する。
非通電の原則を利用する	安全な状態とはエネルギを放出することで得られる。 ある機構の動きが開始される前にエネルギを供給する。 （**JIS B 9700-2，4.11.3** 参照）。 様々なモードについて考察すること。運転モード，保全モードなど。 この原則は特殊な用途に使用することとする。装置の締め付けにエネルギを維持するなど。
適切な留め具	ねじ止めの用途について，製造者の適用ノートを考慮する。十分なトルク負荷技術を適用することで過負荷を防止することができる。
フォース G と同様のパラメータの発生及び／又は通信の限定	例えば，ブレークピン，ブレークプレート，トルク制限クラッチ。
環境パラメータ範囲の制限	パラメータ例としては，温度，湿度，据付場所での汚染。この解説の箇条 **5 e)**の環境要求事項の妥当性確認を参照し，製造者の適用ノートを考慮すること。
速度と同様のパラメータの制限	次を考慮すること。 －　適用に必要な速度，加速度，減速度
適切な反応時間	次を考慮すること。 －　加速減速時のスプリングの疲労，摩擦，注油，温度，慣性，許容値の組み合わせ
予測できない起動の防止	蓄積されたエネルギによって生じる，及び，運転モード，保全モードなどの電源復帰後の予測できない起動を考慮する。 保存されたエネルギの放出に特殊な機器を使用する必要がある場合もある。 特殊なアプリケーション，例えば，装置の締め付け，ポジションの確保に必要なエネルギの保持については別に考慮する必要がある。
簡素化	安全関連システムのコンポーネント数を減らすこと。
分離化	安全関連機能を他の機能と分離する。
適切な注油	－
液体やほこりの侵入を適切に防止する。	IP 定格を考慮する（**IEC 60529** 参照）。

2)　十分吟味された安全原則一覧

解説表 2－十分吟味された安全原則

十分吟味された安全原則	注記
注意して選んだ素材と製造方法を使用する	アプリケーションに関連した適切な素材，十分な製造方法や処理方法を選択すること。
非対称故障モードでコンポーネントを使用する	コンポーネントの主な故障モードは事前に知られており，常に同じである（**JIS B 9700-2**，**4.12.2** 参照）。
オーバーディメンション／安全ファクタ	安全ファクタは基準に準拠する，又は，安全関連アプリケーションに関する十分な経験をもつことで得られる。
安全な位置設定	コンポーネントの可動部分は機械的に設定された位置の一つで保持される（摩擦だけでは不十分）。位置を変更するには力が必要である。
オフ（OFF）力の増加	安全な位置設定／状態はオン（ON）の力に関連してオフ（OFF）の力を増加させることで得ることができる。
アプリケーションに関連したコンポーネント／システムの選択，組み合わせ，配置，組立て，据付を注意深く考える。	－
アプリケーションに関連した締め付け方法を注意深く選ぶこと。	摩擦だけに頼ることを避ける。
ポジティブな機械的動作	部品間の依存運転（パラレル運転など）はポジティブな機械リンクを行うことで得られる。スプリング及び類似の弾性要素はリンクの一部とするべきではない（**JIS B 9700-2**，**4.5** 参照）。
複数の部品	複数の部品を使用することで障害の影響を減らす。（数多くのスプリングのうち）一つのスプリングで一つの障害が発生しても危険な状態にならなくてすむ。
十分吟味されたスプリングの使用（**解説表 3** も参照のこと）	十分吟味されたスプリングには次が必要となる。 －　注意深く選んだ素材，製造方法（使用前に事前設定によるサイクル動作を行う），及び処理（回転，ショットピーニングなど） －　スプリングの十分な誘導 －　疲労応力（破砕が起こる確率が高いなど）に対する十分な安全ファクタ 十分吟味された圧力コイルスプリングも次のように設計する。 －　注意深く選択した素材の使用，製造方法（事前設定してからサイクル動作をさせることで使用するなど），及び処理（回転，ショットピーニングなど） －　スプリングの十分な誘導 －　負荷がかけられていない状態で，ワイヤ直径より少ない角度で旋回する際のクリアランス －　疲労応力（破砕が起こる確率が高いなど）に対する十分な安全ファクタ
力や同様のパラメータの範囲を制限する	経験やアプリケーションに関連して必要な制限を確定する。制限要素の例としては，ブレークピン，ブレークプレート，トルク制限クラッチ。
速度や同様のパラメータの範囲を制限する	経験やアプリケーションに関連して必要な制限を確定する。制限要素の例としては，遠心力調速機，速度とずれの安全モニタリング機能。
環境パラメータの範囲制限	必要な制限を確定する。パラメータ例としては，据付時の温度，湿度，汚染。この解説の箇条 **5 e)**の環境要求事項の妥当性確認を参照し，製造者の適用ノートを考慮すること。
応答時間，制限ヒステリシス（履歴）の範囲制限	必要な制限を確定する。次を考慮すること。 －　スプリングの疲労，摩擦，注油，温度，加速・減速時の慣性，許容値の組み合わせ。

3) 十分吟味されたコンポーネント

解説表 3－十分吟味されたコンポーネント一覧

十分吟味されたコンポーネント	“十分吟味された”の条件	基準又は仕様
ねじ	ねじ接続とアプリケーションに影響する全てのファクタを考慮する。**解説表 2** の十分吟味された安全原則一覧を参照。	ねじ，ナット，座金，リベット，ピン，ボルトなどの機械的接合部品を標準化する。
スプリング	**解説表 2** の十分吟味されたスプリングの使用を参照。	スプリングスチールと他の特殊なアプリケーションの技術仕様は **ISO 4960** で示される。
カム	カム配列に影響する全てのファクタ（インタロック装置の一部）を考慮する。	**JIS B 9710** 参照。
ブレークピン	アプリケーションに影響する全てのファクタを考慮する。**解説表 2** の十分吟味された安全原則一覧を参照。	－

4) 障害一覧と障害の除外

解説表 4－様々な機械装置，コンポーネント，要素
（カムフォロワ，チェーン，クラッチ，ブレーキ，シャフト，ねじ，ピン，ガイド，ベアリングなど）

考慮した障害	障害の除外	注記
磨耗／腐食	規定の寿命に基づいて，注意深く選択した素材，(過) 寸法，製造過程，処理，及び適切な注油を行った場合は，可能（**解説表 2** 参照）。	**JIS B 9705-1**，**7.3** 参照。
緩め	規定の寿命に基づいて，注意深く選択した素材，製造過程，ロックの方法，処理を行った場合は，可能（**解説表 2** 参照）。	
破断	規定の寿命に基づいて，注意深く選択した素材，(過) 寸法，製造過程，処理，及び適切な注油を行った場合は，可能（**解説表 2** 参照）。	
過剰な応力がかかることによる変形	規定の寿命に基づいて，注意深く選択した素材，(過) 寸法，処理，製造過程，及び適切な注油を行った場合は，可能（**解説表 2** 参照）。	
堅さ／粘着度	規定の寿命に基づいて，注意深く選択した素材，(過) 寸法，製造過程，処理，及び適切な注油を行った場合は，可能（**解説表 2** 参照）。	

解説表 5－圧力コイル スプリング

考慮した障害	障害の除外	注記
磨耗／腐食	規定の寿命に基づいて，注意深く選択した素材，(過) 寸法，製造過程，処理，及び適切な注油を行った場合は，可能（**解説表 2** 参照）。	**JIS B 9705-1**，**7.3** 参照。
設定や破断による力の減少		
破断		
堅さ／粘着度		
緩み		
過剰な応力による変形		

b)　ISO 13849-2:2003，附属書 B（参考）空気圧システムの妥当性確認ツール

1)　基本安全原則一覧

解説表 6－基本安全原則一覧

基本安全原則	注記
適した素材と適切な製造方法の採用	次の要素を考慮した素材，製造方法，処理方法の選択。 －　応力，耐性，弾性，摩擦，磨耗，腐食，温度
正しい寸法と形状	次の要素を考慮すること。 －　応力，ひずみ，疲労，表面の粗さ，許容値，製造方法
適切な選択，組み合わせ，配置コンポーネント／システムの組立てと据付	製造者の適用ノート，例えば，カタログシート，据付説明書，仕様書，及び類似のコンポーネント／システムにおけるグッド・エンジニアリング・プラクティスなどを適用する。
非通電の原則を利用する	安全な状態とはエネルギを放出することで得られる。 ある機構の動きが開始される前にエネルギを供給する（**JIS B 9700-2**，**4.11.3** 参照）。 様々なモードについて考察すること。運転モード，保全モードなど。 この原則は特殊な用途に使用することとする。装置の締め付けにエネルギを維持するなど。
適切な締め付け	ねじ留め，留め具，のり付け，クランプリングなどの適用について，製造者の適用ノートを考慮する。 十分なトルク負荷技術を適用することで過負荷を防止することができる。
圧力制限	例えば，圧力放出弁，減圧／制御弁
液体の汚染を十分に防止する	固形粒子と液体の水分のろ過と分離について考察すること。
速度と同様のパラメータの制限	次を考慮すること。 －　適用に必要な速度，加速度，減速度
適切な切り替え時間の範囲	次を考慮すること。 －　配管長，圧力，排気能力，力，スプリングの疲労，磨耗，注油，温度，加速減速時の慣性，許容値の組み合わせ
環境条件への耐性	予測されるあらゆる環境や，予見できる厳しい条件で作動できる機器を設計する。温度，湿度，振動，汚染など。この解説の箇条 **5 e)**の環境要求事項の妥当性確認を参照し，製造者仕様書／適用ノートを考慮すること。
予測できない起動の防止	蓄積されたエネルギによって生じる，及び，運転モード，保全モードなどの電源復帰後の予測できない起動を考慮する。 保存されたエネルギの放出に特殊な機器を使用する必要がある場合もある（**JIS B 9714**，**5.3.1.3** 参照）。 特殊なアプリケーション（クランプ装置のためのエネルギの保持，ポジションの確保など）については別に考慮する必要がある。
簡素化	安全関連システムのコンポーネント数を減らすこと。
適切な温度範囲	システム全体について考察を行うこと。
分離化	安全関連機能を他の機能と分離する。

2) 十分吟味された安全原則

解説表 7－十分吟味された安全原則一覧

十分吟味された安全原則	注記
オーバーディメンショニング／安全ファクタ	安全ファクタは安全関連アプリケーションの基準か十分な経験により得られる。
安全な位置設定	コンポーネントの可動部分は機械的に設定された位置の一つで保持される（摩擦だけでは不十分）。位置を変更するには力が必要である。
オフ（OFF）力の増加	安全な位置設定［オフ（OFF）ポジション］に対するバルブスプールを移動するための領域率は，オン（ON）ポジション（安全ファクタ）にスプールが移動するよりもはるかに大きい。
負荷圧力により弁が閉じる	これらは一般的に，ポペット弁やボール弁などのシート弁である。 壊れた弁を閉じるためにスプリングが閉じても，弁を閉じ続けるためにはいかに負荷圧をかけるかを考慮すること。
ポジティブな機械動作	空気圧コンポーネントの中の可動部品にポジティブな機械動作を使用する。**解説表 2** 参照。
マルチ部品	**解説表 2** 参照。
十分吟味されたスプリングの使用	**解説表 2** 参照。
規定された流量に対して抵抗による速度制限／原則	固定オリフィス，固定スロットルがその例である。
力の制限／力の減少	例えば，十分吟味されたスプリングを備え，正しく寸法を測り，かつ正しく選択した十分吟味された圧力放出弁により実施することが可能。
作動条件の適切な範囲	作動条件の制限。圧力範囲，流量，温度範囲についても考慮する必要がある。
液体の汚染を適切に防止する	固形粒子と液体の水分のろ過と分離について考察すること。
ピストンバルブについて十分なポジティブ結合（重複部分）を確保する	ポジティブの結合部分（重複部分）により，停止機能を確実に得ることができ，また許容できない動作を防ぐことができる。
ヒステリシス（履歴）の制限	例えば，摩擦が増えるとヒステリシス（履歴）が増える。 許容値を組み合わせてもヒステリシスに影響する。

3) 十分吟味されたコンポーネント一覧 現時点では十分吟味されたコンポーネント一覧が提示されていない。十分吟味されたものは，主にアプリケーション限定である。コンポーネントが，**JIS B 9705-1**, **6.2.4** と **EN 983**:1996，箇条 **5**～箇条 **7** に記載された概要説明に準拠していれば，その構成要素は十分吟味されたものと認めることができる。

幾つかのアプリケーションに関する十分吟味されたコンポーネントは，他のアプリケーションに対して適切でない場合もある。

4)　障害一覧と障害の除外

4.1)　各種弁

解説表 8－方向制御弁

考慮する障害	障害の除外	注記
切替回数の変化	作動力が十分である限り，可動コンポーネントにおけるポジティブな機械動作の場合には，可能（**解説表 2** 参照）。	－
切り替えられない（終端又はゼロのポジションで止まっている），又は切り替えが完了しない（動作途中の任意の場所で停止してしまう）	作動力が十分である限り，可動コンポーネントにおけるポジティブな機械動作の場合には，可能（**解説表 2** 参照）。	
最初の切り替えポジションが自発的に変更されてしまう（入力信号なく）	保持力が十分である限り，可動コンポーネントにおけるポジティブな機械動作の場合には，可能（**解説表 2** 参照）。 又は 十分吟味されたスプリングが使われており（**解説表 2** 参照），かつ，正常な据付及び運転条件が適用されている場合には，可能［**注記 1)**参照］。 又は スプール弁にゴム製のバルブが取り付けられ，かつ，正常な据付及び運転条件が適用されている場合には，可能［**注記 1)**を参照］。	**1)**　正常な据付及び運転条件が適用される場合とは， －　製造者が規定した条件が監視され， －　可動部品の重量が，安全上適切な状態で稼動している（水平な据付など）のほか， －　特殊な慣性の力が可動部品にかけられていない（動作方向には，その機械部品の可動方向を考慮するなど） －　衝撃による応力が発生しない
漏れ	スプール形バルブで，ゴム製のシールが取り付けられていることで十分な結合部分（重複部分）が得られている場合［**注記 2)**参照］で，かつ，正常な運転条件が適用され，圧縮空気の処理及びろ過が十分になされている場合には，可能。 又は 通常の運転条件が適用され，かつ，圧縮空気の適切なろ過及び処理を行う場合，シートの使用が可能［**注記 3)**を参照］	**2)**　ゴム製のシールがついたスプール形のバルブの場合には，ろ過による影響はほぼ解決することができる。長時間少量の液漏れが発生している場合を除く。 **3)**　製造者が条件を規定している場合には，通常の運転条件を適用する。
長期間使用することで，液漏れの流量に変化が現れた	なし	－
弁のケースが破裂又は破断し，据付／ケース用のネジが破損／破断している	構造，寸法，据付がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	－
サーボ及びプロポーショナルバルブ。空気圧の障害により，動作が制御できない	サーボ及びプロポーショルバルブの方向指示型で，これらの評価を実施することができる場合には，これらを技術的な安全性に基づいて，設計と構造上これらが一般的な方向指示制御弁である場合には，可能。	－
数多くの単一機能のバルブによって制御機能を実現する場合には，各バルブについて障害分析を実施すること。パイロット弁の場合にも同じ手順を実施する。		

解説表 9－停止（シャットオフ）弁／逆止弁／高速ガス抜き弁／シャトル弁など

考慮する障害	障害の除外	注記
切替回数の変化	なし	－
運転不作動，不完全な開放状態，閉鎖障害又は不完全な閉鎖状態（終端の位置や，動作の中間地点で止まるなど）	可動コンポーネントのガイドシステムが減衰システムをもたない非制御式のボールシート弁と同様に設計されており［**注記 1)**参照］十分吟味されたスプリングが使用されている場合には，可能（**解説表 2** 参照）。	**1)** 減衰システムを備えていない非制御式のボールシート弁については，一般的にガイドシステムが，可動コンポーネントが停止しないような形態で設計されている。
最初の切り替えポジションが自発的に変更されてしまう（入力信号なく）	正常の据付及び運転条件［**注記 2)**参照］で，所定の圧力及び領域を基本として十分な閉鎖力が働いている場合には，可能。	**2)** 正常な据付及び運転条件が適用される場合とは， － 製造者が規定した条件が監視され， － 特殊な慣性の力が可動部品にかけられていない（動作方向には，その機械部品の可動方向を考慮するなど） － 振動や衝撃による過剰な応力が発生しない
シャトル弁について：両側の入力用接合部が同時に閉じてしまう	可動コンポーネントの構造と設計上，同時に閉まることが難しい。	－
漏れ	正常な運転条件が適用され，かつ，圧縮空気の適切なろ過と処理が行われている場合［**注記 3)**を参照］には，可能。	**3)** 製造者が条件を規定している場合には，通常の運転条件を適用する。
長期間の使用中に漏れの流量に変化が現れた	なし	－
弁のケースが破裂又は可動部分が破断する。また，同様に，据付／ケース用のネジが破損／破断する	構造，寸法，据付がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	

解説表 10－フローバルブ

考慮する障害	障害の除外	注記
設定装置を換えていないのに圧力制御機能が変化した	可動部品をもたないフローバルブ，例えば，スロットバルブの場合［**注記 1)**参照］，正常な運転条件を適用し［**注記 2)**参照］，適切なろ過及び処理システムを設置する場合には，可能。	**1)** 設定装置は可動部品としてみなさない。このバルブでは圧力の変化や粘度の変化により流量が変わることは物理的に限界があり，ここで想定する障害として考慮しない。 **2)** 製造者が提示する条件に則していれば正常な運転条件が満たされる。
調節ができない回転式オリフィスとノズルの場合に流量が変化する	直径が≧0.8 mm の場合であり，かつ，正常な運転条件を適用し［**注記 2)**参照］，適切なろ過及び処理システムを設置する場合には，可能。	
プロポーショナル圧力弁:設定値が意図に反して変更されたことで，流量が変化した	なし	

解説表 10－フローバルブ（続き）

考慮する障害	障害の除外	注記
設定装置の自発的な変化	記述的な安全仕様に基づいて特定の事例に対しても設定装置の効果的な保護が行われていれば，可能。	－
設定装置の運転要素のねじが無作為に緩んだ／はずれた	ねじ緩み／はずれに対して効果的なロック装置がある場合には，可能。	
弁のケースが破裂又は可動部分が破損する。また，同様に，据付／ケース用のネジが破損／破断する	構造，寸法，据付方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能	

解説表 11－圧力弁

考慮する障害	障害の除外	注記
設定圧力を超えると（可動部品の動作が固定されている，又は緩慢である［注記 1)参照］，開かない又は十分に開かない（空間的にも，一時的にも）	次の場合，可能。 － 可動部品のガイドシステムが，非制御式のボールシート弁又はメンブレン弁と同様である［注記 2)参照］，例えば，減圧弁に二次的な減圧機能があるか， 及び － 据え付けたスプリングが十分吟味されたスプリングである（**解説表 2** 参照）。	**1)** この障害はクランピングなどの強制的な動作についてだけ適用されるものである。 この障害は圧力制限，減圧などの空気圧システムの通常の機能には適用しない。 **2)** 制御機能をもたないボールシート弁又はメンブレン弁については，そのガイドシステムは，通常，可動部品が固定しにくいように設計されているものである。
圧力が設定値を下回ると開かない又は十分に開かない（空間的にも，一時的にも）（可動部品の動作が固定されている，又は緩慢である［注記 1)参照］		
設定装置を換えていないのに圧力制御機能が変化した［注記 1)参照］	直接作動する圧力制限バルブと圧力切替バルブについては，据え付けられたスプリングが十分吟味されたものである場合には，可能（**解説表 2** 参照）。	
プロポーショナル圧力弁：設定値が意図に反して変更されたことで，圧力制御機能が変化した［注記 1)参照］	なし	
設定装置を換えていないのに圧力制御機能が変化した	特定のアプリケーションの要求事項下にある設定装置に効果的な保護，例えば，漏れシールがある場合には，可能。	－
設定装置の運転要素のねじが無作為に緩んだ／はずれた	ねじ緩み／はずれに対して効果的なロック装置がある場合には，可能。	－
漏れ	通常運転条件［注記 3)参照］において，シート弁，メンブレン弁及びゴム製のバルブがついたスプール弁が使用され，適切な圧縮空気の処理及びフィルタリングが備えられている場合には，可能。	**3)** 通常運転条件とは，製造業者による条件に従った場合に，適合したものとする。
長期使用期間にわたる漏れ流量の変化	なし	－
弁のケースが破裂又は可動部分が破損する。また，同様に，据付／ケース用のネジが破損／破断する	構造，寸法，据付方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	－

4.2) パイプ，ホースアセンブリ及コネクタ

解説表 12－パイプ

考慮する障害	障害の除外	注記
破断と漏れ	寸法測定，素材の選定，固定方法などがグッド・エンジニアリング・プラクティスに基づいている場合には，可能［**注記 1)**を参照］。	**1)** プラスチック製のパイプを使用しているときには，特に運転環境での影響，例えば，熱による影響，化学物質や放熱による影響を加味して，製造者のデータを考慮する必要がある。防食媒体で処理されていないスチールパイプを使用する場合には，圧縮空気による十分な乾燥作業が特に重要になる。
コネクタ障害（例えば，破損，漏れ）	咬合型の取り付け具又はねじ込みパイプ（例えば，スチール製の取り付け具，スチールパイプ）を使用する場合で，寸法，素材の選定，製造方法，構成，固定方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	－
詰まり（遮断）	動力回路での配管については，可能。 公称直径が≧2 mm の場合の制御及び測定配管については，可能。	
公称直径が小さいことによるプラスチックパイプのねじれ	適切に保護され，かつ，据付けられ，最小曲げ半径等製について製造者の関連データも考慮されている場合には，可能。	

解説表 13－ホースアセンブリ

考慮する障害	障害の除外	注記
取り付け具の破断や破損と液漏れ	**ISO 4079-1** に則して製造されたホースを使用したホースアセンブリ，又は，同様のホースで対応するホース取り付け具［**注記 1)** 参照］が取り付けられている場合には，可能。	**1)** 次の場合には障害の除外を考えない。 － 所定の寿命を満了している場合 － 強化部分の疲労が発生している場合 － 外部の損傷が避けられない場合
詰まり（遮断）	動力回路での配管については，可能。 公称直径が≧2 mm の場合の制御及び測定配管については，可能。	－

解説表 14－コネクタ

考慮する障害	障害の除外	注記
ねじの破断や破損又はねじ山の剝がれ	寸法，素材の選定，製造方法，構成，配管及び／又は液体技術部品への接合がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	－
漏れ（気密状態が失われる）	なし［**注記 1)**参照］	**1)** 磨耗，老朽化，弾性の劣化などにより，長期間の障害を除外することができない。気密状態の深刻な障害が突然発生することが想定されていない。
詰まり（遮断）	動力回路での配管については，可能。 公称直径が≧2 mm の場合の制御及び測定配管については，可能。	－

4.3) 圧力トランスミッタ及び圧力媒体トランスデューサ

解説表 15－圧力トランスミッタと圧力媒体トランスデユーサ

考慮する障害	障害の除外	注記
圧力室の気密／油密状態が失われる，又は変化する	なし	－
圧力室の破損と，カバーネジの取り付け部分の破断	寸法，素材の選定，製造方法，構成，固定方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	

4.4) 圧縮空気の処理

解説表 16－フィルタ

考慮する障害	障害の除外	注記
フィルタ要素の遮断	なし	－
フィルタ要素の破断又は部分的な破断	フィルタ要素が十分に圧力に耐えることができれば，可能。	
汚れインジケータ又は汚れモニタの故障	なし	
フィルタケースの破断，又は，カバー又は接続要素の破損	寸法，素材の選定，システムの配置，固定方法がグッド・エンジニアリング・プラクティスに基づいていれば，可能。	

解説表 17－油さし

考慮する障害	障害の除外	注記
設定装置を変更していないのに規定値（ユニット時間に対する油量）が変化した	なし	－
設定装置の自発的な変化	設定装置の効果的な保護が行われ，特定の事例に対しても対応できていれば，可能。	
設定装置の運転要素のねじが無作為に外れた	ねじ外れに対して効果的なロック装置がある場合には，可能。	
ケースの破断又は，カバー又は固定又は接続要素の破損	寸法，素材の選定，システムの配置，固定方法がグッド・エンジニアリング・プラクティスに基づいていれば，可能。	

解説表 18－サイレンサ

考慮する障害	障害の除外	注記
サイレンサの遮断（詰まり）	サイレンサ要素の設計と構造が**注記 1)** の条件を満たしていれば，可能。	**1)** サイレンサ要素の詰まり及び／又は排気の戻り圧が一定の臨界値を超える増加が見られる場合には，サイレンサの直径が十分な大きさではなく，また運転条件に合致するものではない。

4.5)　アキュムレータ及び圧力容器

解説表 19－アキュムレータ及び圧力容器

考慮する障害	障害の除外	注記
アキュムレータ／圧力容器又はコンタクタの破断／破損又は，固定ネジのネジ山ずれ	構造，機器の選定，素材の選定，システムの配置がグッド・エンジニアリング・プラクティスに基づいている場合，可能。	－

4.6)　センサ

解説表 20－センサ

考慮する障害	障害の除外	注記
センサ障害［**注記 1)**を参照］	なし	**1)**　この表のセンサには，特に圧力，流量，温度などについて，信号受信，処理，出力機能が含まれている。
検知能力又は出力特性の変化	なし	－

4.7)　情報処理

解説表 21－論理上の要素

考慮する障害	障害の除外	注記
例えば，切替時間の変化，切替害，又は切替不良などによる論理上の要素に関する障害（例えば，AND，OR，L-S-E 要素）	対応する障害の想定事項や障害の除外については，**解説表 8**，**解説表 9**，**解説表 10** を参照のこと。	－

解説表 22－時間遅延装置

考慮する障害	障害の除外	注記
時間遅延装置，例えば，空気式，及び空気式／機械式時間及びカウント要素の障害 検知能力や出力特性の変化	可動部品をもたない時間遅延装置，例えば，正常の運転条件［**注記 1)**］が適用でき，圧縮空気を適切に処理及びろ過できるような固定抵抗力などがある場合には，可能。	**1)**　製造者から提示された条件に従っている場合，通常の運転条件に適合している。
ケースの破断又は，カバー若しくは固定又は接続要素の破損	構造，素材の選定，据付方法がグッド・エンジニアリング・プラクティスに基づいていれば，可能	－

解説表 23－コンバータ

考慮する障害	障害の除外	注記
コンバータ障害［**注記 1)**参照］ 検知能力と出力特性の変化	可動部品，例えば，リフレックスノズルを備えていないコンバータ，については，正常な運転条件に適合し［**注記 2)** 参照］，圧縮空気が適切に処理，ろ過されている場合には，可能	**1)**　これには，空気圧信号が電気信号に変換されているもの，位置検知（シリンダスイッチ，反射ノズル），空気圧信号の増幅などを含む。 **2)**　製造業者から提示された条件に従っていれば，通常の運転条件に適合したものとみなす。
ケースの破断又は，カバー若しくは固定又は接続要素の破損	構造，素材の選定，据付方法がグッド・エンジニアリング・プラクティスに基づいていれば，可能。	－

c) ISO 13849-2:2003，附属書 C（参考）油圧システムの妥当性確認ツール

1) 基本安全原則

解説表 24－基本安全原則一覧

基本安全原則	注記
適した素材と適切な製造方法の採用	次の要素を考慮した素材，製造方法，処理方法の選択。 － 応力，耐性，弾性，摩擦，磨耗，腐食，温度，油圧液
正しい寸法と形状	次の要素を考慮すること。 － 応力，ひずみ，疲労，表面の粗さ，許容値，製造方法
適切な選択，組み合わせ，配置コンポーネント／システムの組立てと据付	製造者の適用ノート，例えば，カタログシート，据付説明書，仕様書，及び類似のコンポーネント／システムにおけるグッド・エンジニアリング・プラクティスなどを適用する。
非通電の原則を利用する	安全な状態とは，全ての関連する装置に対してエネルギを放出することで得られる。 ある機構の動きが開始される前にエネルギを供給する（**JIS B 9700-2**，**4.11.3** 参照）。 様々なモードについて考察すること。運転モード，保全モードなど。 この原則は，幾つかのアプリケーション，例えば，油圧が失われてしまうと余計な危険状態が発生するようなアプリケーションでは使用しないこと。
適切な締め付け	ねじ留め，留め具，のり付け，クランプリングなどの適用について，製造者の適用ノートを考慮する。 十分なトルク負荷技術を適用することで過負荷を防止することができる。
圧力制限	例えば，圧力放出弁，減圧／制御弁
速度制限／減速	例えば，フローバルブ，又はスロットルによるピストンの速度制限。
液体の汚染を十分に防止する	固形粒子と液体の水分のろ過と分離について考慮すること。 フィルタ保全の必要性を提示するかどうかについても考慮すること。
適切な切替時間の範囲	次を考慮すること。 － 配管の長さ，圧力，排気能力，スプリングの疲労，磨耗，注油，温度／粘土，加速減速時の慣性，許容値の組み合わせ。
環境条件への耐性	予測されるあらゆる環境や，予見できる厳しい条件で作動できる機器を設計する。温度，湿度，振動，汚染など。この解説の箇条 **5 e)**の環境要求事項の妥当性確認を参照し，製造者仕様書／適用ノートを考慮すること。
予測できない起動に対する保護策	蓄積されたエネルギによって生じる，及び，運転モード，保全モードなどの電源復帰後の予測できない起動を考慮する。 蓄積されたエネルギを放出するための特殊な機器が必要な場合もある。 特殊な用途（クランピング装置のためにエネルギを保持したり，位置設定を確定するなど）について別途考察する必要がある。
簡素化	安全関連システムのコンポーネント数を減らすこと。
適切な温度範囲	システム全体で考察する。
分離化	安全関連機能を他の機能と分離する。

2)　十分吟味された安全原則

解説表 25－十分吟味された安全原則一覧

十分吟味された安全原則	注記
オーバーディメンション／安全ファクタ	安全ファクタは基準に準拠する，又は安全関連アプリケーションに関する十分な経験をもつことで得られる。
安全な位置設定	コンポーネントの可動部分は機械的に設定された位置の一つで保持される（摩擦だけでは不十分）。位置を変更するには力が必要である。
オフ（OFF）力の増加	解決策として，バルブスプールを安全な位置に移動すると，その領域率［オフ（OFF）ポジション］はオン（ON）ポジション（安全ファクタ）にスプールを移動するよりもかなり大きくなる。
負荷圧で閉じられた弁	シート弁とカートリッジ弁がその例である。 スプリングで閉じられていた弁が壊れるなどの状態が発生しても，弁を閉じたままの状態にしておくために，負荷圧を適用することを考慮する。
ポジティブな機械的動作	ポジティブな機械的作動は，油圧コンポーネント内の可動部品に対して使用される。**解説表 2** 参照。
複数の部品	**解説表 2** 参照。
十分吟味されたスプリングの使用	**解説表 2** 参照。
定義された流量の抵抗に対して速度を制限／減速	固定オリフィス，固定スロットルがその例である。
力の制限／減力	例えば，十分吟味されたスプリングを備え，正しく寸法を測り，かつ，正しく選択した十分吟味された圧力放出弁により実施することが可能。
作業条件の適切な範囲	圧力計，流量，温度範囲などの作業条件の制限について考慮する。
液体の状態監視	液体中の固形粒子／水を高度にろ過／分離することについて考慮する。 また，液中の化学物質／物理条件についても考慮する。 フィルタ保全の必要性について示す必要があるかどうかについても考慮すること。
ピストン弁での十分なポジティブな結合部分（重複部分）	ポジティブの結合部分（重複部分）により，摩擦がなくなり，許容できない動きを予防することができる。
ヒステリシスの制限	例えば，摩擦が増えるとヒステリシスが増える。許容値を組み合わせてもヒステリシスに影響が出る。

3)　十分吟味されたコンポーネント一覧　現時点では十分吟味されたコンポーネント一覧が提示されていない。十分吟味されたものとなるのは，主にアプリケーション限定である。コンポーネントが，**JIS B 9705-1**，**6.2.4** と **EN 982**:1996，箇条 **5**～箇条 **7** に記載された概要説明に準拠していれば，その構成要素は十分吟味されたものと認めることができる。

4) 障害一覧と障害の除外

4.1) 各種バルブ

解説表 26－方向制御弁

考慮する障害	障害の除外	注記
切替回数の変更	作動力が十分である限り，可動コンポーネントにおけるポジティブな機械動作の場合には，可能（**解説表 2** 参照）。 又は 特殊なタイプのカートリッジシート弁が閉じない場合，少なくとももう一方の弁で液体の主流を制御する場合には，可能［**注記 1)**参照］。	**1)** 次の条件なら特殊なカートリッジシート弁を使用することができる。 － 安全に関連した切替動作を起動する動作領域が，可動部品（ポペット）の 90 %以上であること。 及び － 動作領域での効果的な制御圧力は，該当するシート弁の動作と共に，最大運転圧まで増加させることができる（**EN 982**:1996，**3.5**）。 及び － 可動部品の動作領域とは反対側の領域にかけられている効果的な制御圧力が，最大運転圧力と比べて非常に低い数値である。例えば，圧力ダンプ弁による戻し圧力や，吸引／フィルバルブの供給圧力など。 及び － このシート弁に対するパイロット弁は，マニフォールドブロックを備えるものとして設計されている（ホースアセンブリと，これら弁に接合するパイプはない）。
切り替えられない（終端又はゼロのポジションで止まっている）又は切り替えが完了しない（動作途中の任意の場所で停止してしまう）	作動力が十分である限り，可動コンポーネントにおけるポジティブな機械動作の場合には，可能（**解説表 2** 参照）。 又は 特殊なタイプのカートリッジシート弁が閉じない場合，少なくとももう一方の弁で液体の主流を制御する場合には，可能［**注記 1)**参照］。	
最初の切り替えポジションが自発的に変更されてしまう（入力信号なく）	保持力が十分である限り，可動コンポーネントにおけるポジティブな機械動作の場合には，可能（**解説表 2** 参照）。 又は 十分吟味されたスプリングが使われており（**解説表 2** 参照），かつ，正常な据付及び運転条件が適用されている場合には，可能［**注記 2)**参照］。 又は 特殊なタイプのカートリッジシート弁が閉じない場合，少なくとももう一方の弁で液体の主流を制御し，かつ，通常の据付及び運転条件に適合する場合には，可能［**注記 2)**参照］。	**2)** 正常な据付及び運転条件が適用される場合とは， － 製造者が規定した条件が監視され， － 可動部品の重量が，安全上適切な状態で稼動している（水平な据付など）のほか， － 特殊な慣性の力が可動部品にかけられていない（動作方向には，その機械部品の可動方向を考慮するなど） － 衝撃による応力が発生しない
漏れ	通常の据付及び運転条件が適用され［**注記 3)**参照］，かつ，適切なろ過システムが備えられているシート弁の場合には，可能。	**3)** 製造者が条件を規定している場合には，通常の据付及び運転条件を適用する。

解説表 26－方向制御弁（続き）

考慮する障害	障害の除外	注記
長期間使用することで，液漏れの流量に変化が現れた	なし	－
弁のケースが破裂又は破断し，据付／ケース用のネジが破損／破断している	構造，寸法，据付がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	
サーボ及びプロポーショナルバルブ。空気圧の障害により，動作が制御できない	サーボ及びプロポーショナルバルブの方向指示型で，これらの評価を実施することができる場合には，これらを技術的な安全性に基づいて，設計と構造上これらが一般的な方向指示制御弁である場合には，可能。	
数多くの単一機能のバルブによって制御機能を実現する場合には，各バルブについて障害分析を実施すること。パイロット弁の場合にも同じ手順を実施する。		

解説表 27－停止（シャットオフ）バルブ／逆止弁／シャトル弁など

考慮する障害	障害の除外	注記
切替回数の変化	なし	－
運転不作動，不完全な開放状態，閉鎖障害又は不完全な閉鎖状態（終端の位置や，動作の中間地点で止まるなど）	可動コンポーネントのガイドシステムが減衰システムをもたない非制御式のボールシート弁と同様に設計されており［**注記 1)**参照］十分吟味されたスプリングが使用されている場合には，可能（**解説表 2** 参照）。	**1)** 減衰システムを備えていない非制御式のボールシート弁については，一般的にガイドシステムが，可動コンポーネントが停止しないような形態で設計されている。
最初の切り替えポジションが自発的に変更されてしまう（入力信号なく）	正常の据付及び運転条件［**注記 2)**参照］で，所定の圧力及び領域を基本として十分な閉鎖力が働いている場合には，可能。	**2)** 正常な据付及び運転条件が適用される場合とは， － 製造者が規定した条件が監視され， － 特殊な慣性の力が可動部品にかけられていない（動作方向には，その機械部品の可動方向を考慮するなど） － 振動や衝撃による過剰な応力が発生しない
シャトル弁について：両側の入力用接合部が同時に閉じてしまう	可動コンポーネントの構造と設計上，同時に閉まることが難しい	－
漏れ	正常な運転条件が適用され［**注記 3)**参照］，かつ，適切なろ過システムが備えられている場合には，可能。	**3)** 製造者が条件を規定している場合には，通常の運転条件を適用する。
長期間の使用中に漏れの流量に変化が現れた	なし	－
弁のケースが破裂又は可動部分が破断する。また，同様に，据付／ケース用のネジが破損／破断する	構造，寸法，据付がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	

解説表 28－フローバルブ

考慮する障害	障害の除外	注記
設定装置を換えていないのに圧力制御機能が変化した	可動部品をもたないフローバルブ，例えば，スロットバルブの場合［**注記 1)**参照］，正常な運転条件を適用し［**注記 2)**参照］，かつ，適切なろ過システムを設置する場合には，可能。	**1)** 設定装置は可動部品としてみなさない。このバルブでは圧力の変化や粘度の変化により流量が変わることは物理的に限界があり，ここで想定する障害として考慮しない。 **2)** 製造者が提示する条件に則していれば正常な運転条件が満たされる。
調節ができない回転式オリフィスとノズルの場合に流量が変化する	直径が≧0.8 mm の場合であり，かつ，正常な運転条件を適用し［**注記 2)**参照］，適切なろ過システムを設置する場合には，可能。	
プロポーショナル圧力弁：設定値が意図に反して変更されたことで，流量が変化した	なし	－
設定装置の自発的な変化	記述的な安全仕様に基づいて特定の事例に対しても設定装置の効果的な保護が行われていれば，可能。	
設定装置の運転要素のねじが無作為に緩んだ／はずれた	ねじ緩み／はずれに対して効果的なロック装置がある場合には，可能。	
弁のケースが破裂又は可動部分が破損する。また，同様に，据付／ケース用のネジが破損／破断する	構造，寸法，据付方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	

解説表 29－圧力弁

考慮する障害	障害の除外	注記
設定圧力を超えると（可動部品の動作が固定されている，若しくは緩慢である［**注記 1)**参照］，開かない又は十分に開かない（空間的にも，一時的にも）	特殊なタイプのカートリッジシート弁が閉じない場合には，少なくとももう一方の弁で液体の主流を制御する場合には，可能［**解説表 26 の注記 1)**参照］。 又は 可動コンポーネントに対するガイドシステムが，無制御のボールシート弁と同様に設計されており，ダンピング装置が設けられていない［**注記 2)**参照］うえ，十分吟味されたスプリングが使用されている（**解説表 2** 参照）場合には，可能。	**1)** この障害はクランピングなどの強制的な動作などについてだけ適用されるものである。 障害は圧力制限，減圧などの空気圧システムの通常の機能には適合しない。 **2)** 減衰装置なしの非制御機能タイプのボールシート弁については，ガイドシステムは，通常，可動部品が固着しにくいように設計されているものである。
圧力が設定値を下回ると開かない若しくは十分に開かない（空間的にも，一時的にも）（可動部品の動作が固定されている，又は緩慢である［**注記 1)**参照］		
設定装置を換えていないのに圧力制御機能が変化した［**注記 1)**参照］	直接作動する圧力放出バルブについては，据え付けられたスプリングが十分吟味されたものである場合には，可能（**解説表 2** 参照）。	
プロポーショナル圧力弁:設定値が意図に反して変更されたことで，圧力制御機能が変化した［**注記 1)**参照］	なし	

解説表 29－圧力弁（続き）

考慮する障害	障害の除外	注記
設定装置を換えていないのに圧力制御機能が変化した	技術安全仕様書に関連し，特定の事例において，設定装置が効果的に保護されている場合には，可能（例えば，鉛シール）。	－
設定装置の運転要素のねじが無作為に緩んだ／はずれた	ねじ緩み／はずれに対して効果的なロック装置がある場合には，可能。	
漏れ	通常の運転条件に適合し［注記 3)参照］，適切なろ過システムが備えられている場合には，可能。	3) 製造者が提示する条件に則していれば正常な運転条件が満たされる。
長期使用期間にわたる漏れ流量の変化	なし	－
弁のケースが破裂又は可動部分が破損する。また，同様に，据付／ケース用のネジが破損／破断する	構造，寸法，据付方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	

4.2) 金属配管，ホースアセンブリ，コネクタ

解説表 30－金属配管

考慮する障害	障害の除外	注記
破断と漏れ	寸法測定，素材の選定，固定方法などがグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	－
コネクタ障害（破損，漏れ）	溶接取り付け具又は溶接フランジ，フレア管継ぎ手を使用する場合で，寸法，素材の選定，製造方法，構成，固定方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	
詰まり（遮断）	動力回路での配管については，可能。 公称直径が≧3 mm の場合の制御及び測定配管については，可能。	

解説表 31－ホースアセンブリ

考慮する障害	障害の除外	注記
取り付け具の破断や破損と液漏れ	なし	－
詰まり（遮断）	動力回路での配管については，可能。 公称直径が≧3 mm の場合の制御及び測定配管については，可能。	

解説表 32－コネクタ

考慮する障害	障害の除外	注記
ねじの破断や破損又はねじ山の剝がれ	寸法，素材の選定，製造方法，構成，配管及び／又は液体技術部品への接合がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	－
漏れ（気密状態が失われる）	なし［**注記 1)**参照］	1) 磨耗，老朽化，弾性の劣化などにより，長期間の障害を除外することができない。気密状態の深刻な障害が突然発生することが想定されていない。
詰まり（遮断）	動力回路での配管については，可能。 公称直径が≧3 mm の場合の制御及び測定配管については，可能。	－

4.3) フィルタ

解説表 33－フィルタ

考慮する障害	障害の除外	注記
フィルタ要素の遮断	なし	－
フィルタ要素の破断	フィルタ要素が十分に圧力に耐えることができ，効率的なバイパス弁や効率的な汚れ監視機能があれば，可能。	
バイパス弁の障害	バイパス弁のガイドシステムが，無制御のボールシート弁と同様に設計されており，ダンピング装置が設けられていない（**解説表 27** 参照）うえ，十分吟味されたスプリングが使用されている（**解説表 2** 参照）場合には，可能。	
汚れインジケータ又は汚れモニタの障害	なし	
フィルタケースの破断又は，カバー若しくは接続要素の破損	寸法，素材の選定，システムの構成，固定方法がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	

4.4) エネルギストレージ

解説表 34－エネルギストレージ

考慮する障害	障害の除外	注記
エネルギストレージ容器又はコネクタ，若しくはカバーネジの破断／破損と，ネジ山のすれ	構成，機器の選定，素材の選定，システムの構成がグッド・エンジニアリング・プラクティスに基づいている場合には，可能。	－
ガスと作動液を分離する要素で漏れが生じている	なし	－
ガスと作動液を分離する要素が破断／破損している	シリンダ／ピストンストレージ［**注記 1)**参照］の場合には，可能。	1) 突然発生する大規模な漏れは考慮しない
ガス側のフィリングバルブの障害	フィリングバルブがグッド・エンジニアリング・プラクティスに基づいており，また外的な影響から適切に保護されている場合には，可能。	－

4.5)　センサ

解説表 35－センサ

考慮する障害	障害の除外	注記
センサ障害［**注記 1)**を参照］	なし	1)　この表のセンサには，特に圧力，流量，温度などについて，信号受信，処理，出力機能が含まれている。
検知能力又は出力特性の変化	なし	－

d)　ISO 13849-2:2003，附属書 D（参考）電気システムの妥当性確認ツール

1)　基本安全原則

解説表 36－基本安全原則一覧

基本安全原則	注記
適した素材と適切な製造方法の採用	次の要素を考慮した素材，製造方法，処理方法の選択。 －　応力，耐性，弾性，摩擦，磨耗，腐食，温度
正しい寸法と形状の測定	次の要素を考慮すること。 －　応力，耐性，弾性，摩擦，磨耗，腐食，温度
適切な選択，組み合わせ，配置コンポーネント／システムの組立てと据付	製造者の適用ノート，例えば，カタログシート，据付説明書，仕様書，グッド・エンジニアリング・プラクティスなどを適用する。
正しい保護ボンディング	制御回路の一方，各電磁装置の作業コイルの一端，又は他の電気装置の 1 終端を，保護された接着回路に接続する（全体的な解説については **JIS B 9960-1，9.4.3.1** を参照）。
絶縁状態の監視	接地障害を示すか，接地障害が発生した後に回路を自動的に遮断する，絶縁監視装置を使用（**JIS B 9960-1，6.3.3** を参照）
非通電の原則を利用する	安全な状態とは全ての関連装置の通電を解除することで得られる。例えば，入力については常時閉鎖（NC）接点（押しボタンとポジションスイッチ）と，常時開放（NO）接点をリレーする（**JIS B 9700-2，4.11.3** 参照）。例外も存在している。例えば，電源が落ちると更なる危険な状態が生じるなどである。システムの安全な状態を達成するには時間遅延機能も必要である（**JIS B 9960-1，9.2.2** 参照）。
過渡電流の抑制	抑制装置（RC，ダイオード，バリスタ）を負荷に対して平行に使用する。接点に対して平行ではない。 ダイオードはスイッチを切る時間を増加させる。
応答時間の減少	切替部品の非通電においては遅延を最小限に抑える。
環境条件への対応	全ての想定される環境と，予見される危機的条件［例えば，温度，湿度，振動，電磁障害（EMI）］において作動する機器を設計すること［この解説の箇条 **5 e)**の環境要求事項の妥当性確認参照］。
入力装置の固定	入力装置，例えば，インタロックスイッチ，ポジションスイッチ，リミットスイッチ，近接スイッチ等を固定する。これによりポジション，配列，切替誤差を，全ての想定条件（例えば，振動，正常な磨耗，異物の進入，温度など）で維持することができる。 **JIS B 9710，箇条 5** 参照。
予測できない起動の防止	予測できない起動（例えば，電源復帰後など）を防止する（**JIS B 9700-2，4.11.4，JIS B 9714，JIS B 9960-1** を参照）。
制御回路の保護	制御回路は **JIS B 9960-1，7.2** 及び **9.1.1** 参照。
冗長信号のシリアル接点の回路について一連の切替操作	両方の接点の溶接障害の共通モード，切替操作が同時に行われないように，接点は常に通電しない状態で切替を行う。

2) 十分吟味された安全原則

解説表 37－十分吟味された安全原則一覧

十分吟味された安全原則	注記
ポジティブな機械的結合接点	ポジティブな機械的結合接点を利用する。例えば，監視機能に対して（**JIS B 9700-2**，**4.5** 参照）。
ケーブルの障害回避	二つの隣接するコンダクタの短絡を回避する。 － 各コンダクタに取り付けられている保護回路にシールドを接続したケーブルを使用する － フラットケーブルにおいて，信号コンダクタの間に，接地したコンダクタを使用する
距離	ポジション端末，コンポーネント，配線は十分な距離をもって配置し，所定外の接続を防止する。
エネルギ制限	エネルギの有限量を提供するためにコンデンサを使用する。タイマーアプリケーションなど。
電気パラメータの制限	電源，電流，エネルギ又は周波数の制限：トルグ制限，変位／時間制限を設けた保持・実行の手順，減速など。非安全な状態を防止することを目的としている。
定義されていない状況が発生しないこと	制御システムに非定義な状態が発生するのを避けること。制御システムは，通常の運転や全ての想定される運転条件，例えば，その出力が予見される状態において作動するように設計，構築すること。
ポジティブモードでの作動	弾性要素はなく，形状（強度ではない）により直接の動作を伝達する。例：アクチュエータとコンタクタの間のスプリング（**JIS B 9714**，**5.1** 参照）。
非対称故障モード	コンポーネントやシステムの非対称故障モードは実現可能な限り使用すること。**JIS B 9700-2**，**4.12.2** 参照。
オーバーディメンション	安全回路で使用されているコンポーネントの出力を下げる。例えば， － 切り替えた接点を通る電流は，定格電流の半分に満たないこととする － コンポーネントの切替頻度は，各定格値の半分に満たないこととする － 予測される切替操作の総数は装置の電気耐性の 10 分の 1 未満とする **注記** 出力減少については，それぞれの設計規定による。
障害の可能性を最小限に抑える	安全関連機能は他の機能から分離しておくこと。
複雑性／簡素性のバランス	バランスは次の関係を考慮する。 － よりよい制御機能を達成するための複雑性 及び － より高い信頼度を得るための容易性

3) 十分吟味されたコンポーネント

解説表 38－十分吟味されたコンポーネント一覧

十分吟味されたコンポーネント	“十分吟味された”に関する追加条件	基準又は仕様
ポジティブモード作動（直接的な開放動作）での切替，例えば， － 押しボタン － ポジションスイッチ － カム操作セレクタスイッチ モード操作など	－	**JIS C 8201-5-1，附属書 K**
非常停止装置	－	**JIS B 9703**
ヒューズ	－	**JIS C 8269-1**
サーキットブレーカ	－	**IEC 60947-2**
変位サーキットブレーカ／RCD（残留電流の検知）	－	**IEC 60947-2，附属書 B**
メインコンタクタ（主接触器）	次の条件を満たすものだけ十分吟味されたものとみなす。 **a)** 他の影響を考慮に入れる，例えば，振動など **b)** 適切な方法による障害防止，例えば，オーバーディメンションなど（**解説表 37** など） **c)** 熱保護装置により電流に負荷が掛かるのを制限する 過負荷に対して，保護装置で回路を保護する。	**IEC 60947-4-1**
制御及び保護切替装置又は機器（CPS）	－	**IEC 60947-6-2**
補助コンタクタ（コンタクタリレーなど）	次の条件を満たすものだけ十分吟味されたものとみなす。 他の影響を考慮に入れる，例えば，振動など ポジティブな通電動作 適切な方法による障害防止， 例えば，オーバーディメンションなど（**解説表 37** など） 接点の電流はヒューズか回路ブレーカーで制限され，接点の溶接を防止する 接点を監視用に使用する際には，ポジティブな機械的ガイドとする。	**EN 50205** **JIS B 9960-1** **JIS C 8201-5-1**
トランスフォーマ	－	**JIS C 61558**
ケーブル	きょう体に外付するケーブルは，機械的な損傷から保護する（振動又は曲げを含む）。	**JIS B 9960-1，箇条 12**
プラグとソケット	－	所定のアプリケーションに関する電気基準に基づく。 インタロックに関しては，**JIS B 9710** も参照。
温度スイッチ	－	電気側については，**JIS C 8201-5-1，附属書 K** 参照。

解説表 38－十分吟味されたコンポーネント一覧（続き）

十分吟味されたコンポーネント	“十分吟味された”に関する追加条件	基準又は仕様
圧力スイッチ	－	電気側については，**JIS C 8201-5-1**，附属書**K**を参照。 圧力側については，解説の箇条 **5 b)**及び箇条 **5 c)**参照。
電磁弁	－	－

4)　障害一覧と障害の除外

4.1)　コンダクタ及びコネクタ

解説表 39－コンダクタ／ケーブル

考慮する障害	障害の除外	注記
二つのコンダクタ間での短絡	次のコンダクタ間での短絡， －　恒久的な接続（固定）と外部からの障害に対する保護，例えば，ケーブルダクト，アーマーなどによる －　別々のマルチコアケーブル －　電気きょう体内に収容する［**注記 1)**を参照］ －　接地接続で個々にシールドする	**1)**　コンダクタときょう体両方が適切な要求事項を満たしていること（**JIS B 9960-1** 参照）。
コンダクタと露出する伝導部品又は，アース又は，保護固定コンダクタ間での短絡	電気きょう体内においてコンダクタと露出する伝導部品間で起こる短絡［**注記 1)**参照］	
コンダクタの開放回路	なし	－

解説表 40－プリント回路盤／アセンブリ

考慮する障害	障害の除外	注記
二つの隣接する軌道／パッド間の短絡	**注記 1)**～**注記 3)**に基づき，隣接するコンダクタ間での短絡	**1)**　使用した基盤は **IEC 61249-2** に従うものであり，沿面距離とクリアランスは少なくとも，汚染度 2／据付種別 III で **JIS C 60664-1** の寸法となる。 **2)**　アセンブルボードの印字面は老朽化防止のワニスをかけてあるか，**JIS C 60664-3** による全てのコンダクタパスを保護層でカバーしている。 **3)**　離れた場所での据付台を含む，制御システムの安全関連部の全てのきょう体は，規定の通り据付けた状態で少なくとも IP54 の保護性能をもっていることとする（**JIS C 0920** 参照）。
開放回路	なし	－

解説表 41－端子台

考慮する障害	障害の除外	注記
隣接する端子間の短絡	**注記 1)**又は**注記 2)**に基づいた隣接する端子間の短絡	**1)** 使用した端子は IEC 基準及び，**JIS B 9960-1**，**13.1.1** を満たすものとする。 **2)** これら自体が，短絡を防止するように設計されている。例えば，接続点の上にプラスチックのチューブをまとめてあるなど。
個々の端子の開放回路	なし	－

解説表 42－マルチピンコネクタ

考慮する障害	障害の除外	注記
二つの隣接したピンの間の短絡	**注記 1)**又は**注記 2)**に基づいた隣接するピンの間の短絡	**1)** 複数のワイヤを束ねるには止め輪（フェルール）か他の適当な方法を用いる。沿面距離とクリアランス，及び，全ての間隔は，少なくとも **JIS C 60664-1**，据付種別 III を満たすこととする。 **2)** アセンブルドボードは少なくとも IP54（**JIS C 0920** 参照）のきょう体内に据え付けるものであり，アセンブルドボードの印字面は経年変化を防止するワニスをかけてあるか，**JIS C 60664-3** に基づいて全てのコンダクタパスが保護層でカバーされていることとする。
機械的な手段によって保護されてなかったため，コネクタが入れ替えられた，又は誤って挿入された	なし	－
コンダクタ［**注記 3)**参照］と接地，又は伝導部品から保護コンダクタまでの短絡	なし	**3)** ケーブル芯はマルチピンコネクタの一部としてみなす。
個々のコネクタピンの開放回路	なし	－

4.2) スイッチ

解説表 43－電子機械式ポジションスイッチ，手動操作用スイッチ（例えば，押しボタン，リセットアクチュエータ，DIP スイッチ，磁気操作接点，リードスイッチ，圧力スイッチ，温度スイッチなど）

考慮する障害	障害の除外	注記
接点が閉じない	なし	－
接点が開かない	**JIS C 8201-5-1**，**附属書 K** に基づく接点であれば，開くと期待される。	－
互いに絶縁した隣接する接点間で短絡が起きている	**JIS C 8201-5-1** に基づくスイッチに対しては短絡を除外することができる［**注記 1)**参照］。	**1)** 緩慢になる伝導部品は接点間の絶縁の橋渡しをするものではない。
切替接点の三つの端子間で同時に短絡が起きている	同時に発生した短絡は，**JIS C 8201-5-1** に基づくスイッチに対しては除外することができる［**注記 1)**参照］。	
機械的な観点からみた障害の一覧は，この解説の箇条 **5 a)**にて考察する。		

解説表 44－電子機械装置（例えば，リレー，コンタクタリレーなど）

考慮する障害	障害の除外	注記
コイルが通電していない状態で，全ての接点が通電し続けている（機械的な障害など）	なし	－
電源を投入した時点で，全ての接点が通電していない（機械的な障害，コイルの開放回路などによる）	なし	
接点が開いていない	なし	
接点が閉じてない	なし	
切替接点の三つの端末間で同時に短絡が起きている	同時に発生した短絡は，**JIS C 8201-5-1** に基づくスイッチに対しては除外することができる［**注記 1)**参照］。	**1)** 沿面とクリアランスの距離は，少なくとも **JIS C 60664-1** で，汚染度 2／据付種別 III を満たすこととする。
2 対の接点及び／又は複数の接点とコイル端子の間で短絡が起こっている	**注記 1)**及び**注記 2)**の条件が満たされれば，短絡は除外される。	**2)** 緩慢になった伝導部品は接点とコイルの間の絶縁を橋渡しすることはできない。
NO 接点と NC 接点が同時に閉鎖した	**注記 3)**の条件が満たされていれば，接点が同時に閉じる問題は除外することができる。	**3)** ポジ底部に作動した（又は機械的にリンクした）接点を使用する。

解説表 45－近接スイッチ

考慮する障害	障害の除外	注記
出力の抵抗値が常に低い	なし［**注記 1)**参照］	**1)** **IEC 60947-5-3** 参照。
出力の抵抗値が常に高い	なし［**注記 2)**参照］	**2)** 障害防止策について解説する必要がある。
電源に障害が発生している	なし	－
機械障害により，スイッチが作動しない	**注記 3)**が満たされていれば，機械の障害による運転はない。	**3)** スイッチの全ての部品は十分に固定する必要がある。機械的な観点については，解説の箇条 **5 a)**を参照。
切替接点の三つの端子間で短絡が起きている	なし	－

解説表 46－電磁弁

考慮する障害	障害の除外	注記
通電しない	なし	－
通電が切れない	なし	
空気圧及び油圧弁の機械的な観点からみた障害の一覧については，解説の箇条 **5 b)**及び箇条 **5 c)**にてそれぞれ考察している。		

4.3)　ディスクリート電気コンポーネント

解説表 47－トランスフォーマ

考慮する障害	障害の除外	注記
個々の巻き線で回路が開いている	なし	－
異なる複数の巻き線で短絡が起きている	様々な巻き線間での短絡は，**注記 1)**の条件が満たされれば除外できる。	**1)**　**JIS C 61558** の要求事項を満たすこととする。500 V 未満の定格電圧に対して，絶縁は 2 500 Va.c.テスト電圧の要求事項を満たすこととする。コイルや巻き線での短絡は，次の対策を講じることで回避する必要がある。 －　含芯コイルを利用することで，各コイル間や，コイル本体と芯の間の空洞を全て埋めることができる。 －　巻き線コンダクタを使用することで，絶縁と高熱定格を十分に満たすことができる。 **2)**　2 次的な短絡でも，規定の運転温度を超えて発熱しないようにする。
一つの巻き線で短絡が起きている	一つ巻き線間での短絡は，**注記 1)**の条件が満たされれば除外できる。	
効率的な回転率が変化する	**注記 1)**の条件が満たされれば，効果的な回転率が変化するという障害は除外できる。**注記 2)**のガイダンスも参照。	

解説表 48－インダクタンス

考慮する障害	障害の除外	注記
開放回路	なし	－
短絡	**注記 1)**の条件が満たされれば短絡は除外することができる。	**1)**　コイルは 1 層で，エナメル又はポット加工したもの，また軸ワイヤ接続と軸に据付。
数値がランダムに変わる 0.5Ln＜L＜Ln+許容誤差 Ln がインダクタンスの定格値である場合［**注記 2)**を参照］	なし	**2)**　構造の種類によっては他の範囲を考慮することができる。

解説表 49－抵抗器

考慮する障害	障害の除外	注記
開放回路	なし	－
短絡	**注記** 1)の条件が満たされれば短絡は解消される。 表面据付技術により使用した抵抗器については障害を解消できない。	1) 抵抗器はフィルムタイプ又は，破損時にワイヤの巻き戻りを保護するワイヤ巻きタイプ，軸ワイヤ接続，軸据付，ワニスがけしてある。
数値がランダムに変わる 0.5Rn＜R＜2Rn Rn が抵抗値の定格値である場合［**注記** 2)を参照］	なし	2) 構造の種類によっては他の範囲を考慮することができる。

解説表 50－抵抗器ネットワーク

考慮する障害	障害の除外	注記
開放回路	なし	－
二つの接続間の短絡	なし	
任意の接続間の短絡	なし	
数値がランダムに変わる 0.5Rn＜R＜2Rn Rn が抵抗値の定格値である場合［**注記** 1)を参照］	なし	1) 構造の種類によっては他の範囲を考慮することができる。

解説表 51－電位差計

考慮する障害	障害の除外	注記
個々の接続での開放回路	なし	－
全ての接続間での短絡	なし	
二つの接続間での短絡	なし	
数値がランダムに変わる 0.5Rp＜R＜2Rp Rp が抵抗値の定格値である場合［**注記** 1)を参照］	なし	1) 構造の種類によっては他の範囲を考慮することができる。

解説表 52－コンデンサ／キャパサイタ

考慮する障害	障害の除外	注記
開放回路	なし	－
短絡	なし	
数値がランダムに変わる 0.5Cn＜C＜2Cn+許容誤差 Cn が抵抗値の定格値である場合［**注記** 1)を参照］	なし	1) 構造の種類によっては他の範囲を考慮することができる。
Tan δ 値が変わる	なし	－

4.4) 電子コンポーネント

解説表 53－ディスクリート半導体
［例えば，ダイオード，ツェナーダイオード，トランジスタ，トライアック（サイリスタ），電圧調整器，クオーツクリスタル，フォトトランジスタ，発光ダイオード（LED）など］

考慮する障害	障害の除外	注記
任意の接続における開放回路	なし	－
二つの接続間の短絡	なし	
全ての接続間の短絡	なし	
特性の変化	なし	

解説表 54－オプトコプタ

考慮する障害	障害の除外	注記
個々の接続の開放回路	なし	－
二つの入力接続間の短絡	なし	
二つの出力接続間の短絡	なし	
入出力の二つの接続間での短絡	入出力間での短絡は，**注記 1)**が満たされれば除外することができる。	**1)** 基盤は **IEC 61249-2** に基づくものとし，沿面距離とクリアランスは少なくとも **JIS C 60664-1** の汚染度 2／据付種別 III とする。

解説表 55－プログラミング不用の集積回路

注記 1 この基準においては，1 000 ゲート及び／又は 24 ピン未満の IC，操作用アンプ，シフトレジスター，ハイブリッドモジュールは複合体としてみなさない。この定義は，任意のものである。

考慮する障害	障害の除外	注記
各接続部での開放回路	なし	－
二つの接続間での短絡	なし	
単一の縮退故障（例えば，絶縁された入力側か，切断された出力側で 1 又は 0 に短絡するなど）。0 や 1 の静的信号は，個々に，若しくは，同時に全ての入出力側で発生し得る。	なし	－
出力の寄生振動	なし	
数値の変化（例えば，アナログ装置の入出力電圧など）	なし	

解説表 56－プログラマブル及び／又は複合集積回路

注記 2 この基準においては，1 000 ゲート及び／又は 24 ピン以上の IC，操作用アンプ，シフトレジスター，ハイブリッドモジュールは複合体としてみなす。この定義は，任意のものである。分析により，安全機能の操作に影響を及ぼしかねない障害を更に特定していくのが望ましい。

考慮する障害	障害の除外	注記
ソフトウェアの障害を含む，機能の全て，又は，その一部の障害	なし	－
個々の接続の開放回路	なし	
二つの接続間での短絡	なし	
単一縮退故障（絶縁された入力側か，切断された出力側で 1 と 0 に短絡するなど）。0 や 1 の静的信号は，個々に，若しくは，同時に全ての入出力側で発生し得る。	なし	
出力の寄生振動	なし	
数値の変化（アナログ装置の入出力電圧など）	なし	
集積回路の複雑性により，検知しにくいハードウェアの障害が検知されない。	なし	

e) **環境要求事項の妥当性確認** 制御システムの安全関連部に関して設計で指定した性能は，制御システムに対して指定した環境条件に照らして妥当性確認を実施する必要がある。

妥当性確認は，分析により，又は必要に応じて試験によって実施される。

分析及び試験の範囲は，安全関連部，これらが据付けられるシステム，使用する技術，妥当性確認がなされる環境条件に左右される。システム及びそのコンポーネントに関する運転上の信頼性データを使用したり，適切な環境基準への準拠性を確認する（防水，耐振性など）ことで，この妥当性確認手順を補足することができる場合もある。

適切な場合，妥当性確認を検討する項目を，次に示す。

－ 衝撃，振動，汚染物質の進入による，予想される機械に対するストレス
－ 機械的耐性
－ 定格と電源
－ 気象条件（温度と湿度）
－ 電磁両立性（イミュニティ）

環境要求事項への準拠性を決定するために試験が必要な場合，用途に合わせて関連する規格に記載された手順で実行される。

試験による妥当性確認が終了したら，安全機能が継続して安全要求事項の仕様書に基づく必要がある。又は制御システムの安全関連部は，安全状態の出力を生成する必要がある。

6 原案作成委員会の構成表

原案作成委員会の構成表を，次に示す。

JIS B 9705-1 原案作成委員会　構成表

	氏名	所属
(委員長)	杉本　旭	長岡技術科学大学専門職大学院
(副委員長)	山田陽滋	名古屋大学
(委員)	向殿政男	明治大学
	平野由紀夫	経済産業省
	安達　栄	厚生労働省
	池田博康	独立行政法人労働安全衛生総合研究所
	井上洋一	ビューロベリタス
	杉田吉広	テュフラインランドジャパン株式会社
	石川滋久	テュフズードジャパン株式会社
	山本元芳	社団法人日本工作機械工業会
	三浦敏道	社団法人日本ロボット工業会
	大村宏之	社団法人日本食品機械工業会
	蓬原弘一	明治大学
	横井孝志	独立行政法人産業技術総合研究所
	中嶋洋介	武蔵野大学
	杉原健治	パナソニックファクトリーソリューションズ株式会社
	平沼栄浩	セーフティープラス株式会社
	高橋克知	ブリヂストン株式会社
	宮川光雄	トヨタ自動車株式会社
	内藤博光	ソニーファシリティマネジメント株式会社
	内藤信吾	株式会社ダイフク研究・研修センター
	中谷英司	株式会社 SOKUDO
	金友正文	株式会社日立製作所
	石川　篤	住友重機械工業株式会社
	浦島　直	三菱重工業株式会社
	坂田文彦	株式会社荏原製作所
	木下博文	平田機工株式会社
	永田　学	株式会社神戸製鋼所
	山谷光一	株式会社牧野フライス製作所
	井上正也	オムロン株式会社
	長谷川佳宣	SUNX 株式会社
	関野芳雄	IDEC 株式会社
(事務局)	宮崎浩一	社団法人日本機械工業連合会

JIS B 9705-1 原案作成 WG　構成表

	氏名	所属
(主査)	蓬 原 弘 一	明治大学
(委員)	杉 本 　 旭	長岡技術科学大学専門職大学院
	向 殿 政 男	明治大学
	池 田 博 康	独立行政法人労働安全衛生総合研究所
	山 本 正 宣	日本大学
	石 川 滋 久	テュフズードジャパン株式会社
	平 沼 栄 浩	セーフティープラス株式会社
	鈴 木 　 央	テュフラインランドジャパン株式会社
	坂 井 正 善	日本信号株式会社
	中 谷 英 司	株式会社 SOKUDO
	羽 田 健 一	株式会社明電舎
	長谷川 佳 宣	SUNX 株式会社
	関 野 芳 雄	IDEC 株式会社
	黒 住 光 男	ジック株式会社
	井 上 正 也	オムロン株式会社
	杉 原 健 治	パナソニックファクトリーソリューションズ株式会社
	柵 木 勝 博	株式会社ジェイテクト
	大 橋 功 治	ヤマザキマザック株式会社
	篠 木 富二生	三菱重工業株式会社
(事務局)	宮 崎 浩 一	社団法人日本機械工業連合会

(執筆者　宮崎　浩一)

白　紙

★JIS 規格票及び JIS 規格票解説についてのお問合せは，規格開発部標準課まで，できる限り電子メール（E-mail:sd@jsa.or.jp）又は FAX［(03)3405-5541］TEL［(03)5770-1571］でお願いいたします。お問合せにお答えするには，関係先への確認等が必要なケースがございますので，多少お時間がかかる場合がございます。あらかじめご了承ください。

★JIS 規格票の正誤票が発行された場合は，次の要領でご案内いたします。

(1) 当協会発行の月刊誌“標準化と品質管理”に，正・誤の内容を掲載いたします。

(2) 原則として毎月 21 日（21 日が土曜日，日曜日又は休日の場合には，その翌日）に，“日経産業新聞”及び“日刊工業新聞”の JIS 発行の広告欄で，正誤票が発行された JIS 規格番号及び規格の名称をお知らせいたします。

なお，当協会の JIS 予約者の方には，予約されている部門で正誤票が発行された場合，自動的にお送りいたします。

★JIS 規格票のご注文は，出版事業部出版サービス第一課［FAX(03)3583-0462 TEL(03)3583-8002］まで，お申込みください。

JIS B 9705-1（ISO 13849-1）
機械類の安全性－制御システムの安全関連部－第 1 部：設計のための一般原則

平成 23 年 8 月 1 日　第 1 刷発行

編集兼
発行人　田 中 正 躬

発 行 所

財団法人 日 本 規 格 協 会
〒107-8440　東京都港区赤坂 4 丁目 1-24
http://www.jsa.or.jp/

札 幌 支 部　〒060-0051　札幌市中央区南 1 条東 1 丁目 5　大通バスセンタービル 1 号館内
TEL (011)261-0045　FAX (011)221-4020

名古屋支部　〒460-0008　名古屋市中区栄 2 丁目 6-1　白川ビル別館内
TEL (052)221-8316(代表)　FAX (052)203-4806

関 西 支 部　〒541-0053　大阪市中央区本町 3 丁目 4-10　本町野村ビル内
TEL (06)6261-8086(代表)　FAX (06)6261-9114

広 島 支 部　〒730-0011　広島市中区基町 5-44　広島商工会議所ビル内
TEL (082)221-7023　FAX (082)223-7568

福 岡 支 部　〒812-0025　福岡市博多区店屋町 1-31　博多アーバンスクエア内
TEL (092)282-9080　FAX (092)282-9118

Printed in Japan　DI

JAPANESE INDUSTRIAL STANDARD

Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design

JIS B 9705-1 : 2011

(ISO 13849-1 : 2006)

(JMF)

Revised 2011-07-25

Investigated by

Japanese Industrial Standards Committee

Published by

Japanese Standards Association

定価 4,620 円（本体 4,400 円）

ICS 13.110

Reference number：JIS B 9705-1:2011(J)